IEEE802.11n Industrial Access Point, W/802.3af POE

Manual Ver 0.0.1 WAP-854NP

Table of Contents

Chapter 1. Before You Start 1

1.1 Preface 1

1.2 Package Contents 1

Chapter 2. System Overview 2

2.1 Introduction of WAP-854NP 2

2.2 Specification 3

Chapter 3. Base Installations 6

3.1 Installations 6

3.1.1 System Requirements 6

3.1.2 Panel Function Descriptions 6

3.1.3 Hardware Installation 8

3.2 Software Configuration 9

3.2.1 Getting Start 9

3.2.2 Quick Configuration 11

Chapter 4. AP Mode Configuration 13

4.1 Connect WAP-854NP to the Wired Local Network 14

4.1.1 Network Requirement 14

4.1.2 Configure LAN Port 15

4.2 Create Your Wireless Network 17

4.2.1 Configure Wireless General Setup 17

4.2.2 Configure Wireless Advanced Setup 19

4.2.3 Create Virtual AP 22

4.2.3.1 Configure Virtual AP 24

4.2.3.2 Block Wireless Clients 30

4.2.3.3 Monitor Associated Wireless Clients 31

4.3 Expand Your Wireless Network 32

4.3.1 Create WDS Link 32

4.3.2 View WDS Link Status 33

4.4 Manage the System 34

4.4.1 Configure System Time 34

4.4.2 Configure Management 35

4.4.3 Configure SNMP 37

4.4.4 Backup / Restore and Reset to Factory 38

4.4.5 Firmware Upgrade 39

4.4.6 Network Utility 40

4.4.7 Reboot 41

4.5 Observer the Status 42

4.5.1 Overview 42
4.5.2 Extra Info 43
4.5.3 Event Log 45
Chapter 5. WDS Mode Configuration 46
5.1 Connect WAP-854NP to the Wired Local Network 46
5.1.1 Network Requirement 46
5.1.2 Configure LAN Port 47
5.2 Expand Your Wireless Network 49
5.2.1 Configure Wireless General Setup 49
5.2.2 Configure Wireless Advanced Setup 51
5.2.3 Create WDS Link 54
5.2.4 View WDS Link Status 55
5.3 Manage the System 56
5.3.1 Configure System Time 56
5.3.2 Configure Management 57
5.3.3 Configure SNMP 59
5.3.4 Backup / Restore and Reset to Factory 60
5.3.5 Firmware Upgrade 61
5.3.6 Network Utility 62
5.3.7 Reboot 63
5.4 Observer the Status 64
5.4.1 Overview 64
5.4.2 Extra Info 65
5.4.3 Event Log 67
Appendix A. Web GUI valid Characters 68

Chapter 1. Before You Start

1.1 Preface

Aspiring to provide the best performance/price ratio for both SMB and industrial applications, WAP-854NP is uniquely designed for Wall Mount with metal case and IP50 rating for a fast, robust, secure and business class access point perfect for installation in factories, warehouses, hotels marinas, hospitals, large homes, hotspot and more.

WAP-854NP is compliant to the latest wireless standards that are required in highly secured enterprise networking environments. Its Wireless Distribution System (WDS) feature allows for flexible extension of wireless coverage. It can be power via three alternative methods from either the Single LAN port for Power over Ethernet (PoE), DC jack providing the ability to back up each other with fail-over redundancy function, giving WAP-854NP reliable connectivity in mission critical situations.

1.2 Package Contents

Package Contents

• WAP-854NP	x 1
• CD-ROM (with User Manual and QIG)	x 1
• Console Cable	x 1
• Ethernet Cable	x 1
• Power Adapter DC12V 1A	x 1
• Antenna	x 2
• Ground Cable	x 1
• Mounting Kit	x 1

It is highly recommended to use all the supplies in the package instead of substituting any components by other suppliers to guarantee best performance.

Chapter 2. System Overview

2.1 Introduction of WAP-854NP

Aspiring to provide the best performance/price ratio for both SMB and industrial applications, WAP-854NP is uniquely designed for Wall Mount with metal case and IP50 rating for a fast, robust, secure and business class access point perfect for installation in factories, warehouses, hotels marinas, hospitals, large homes, hotspot and more.

WAP-854NP is compliant to the latest wireless standards that are required in highly secured enterprise networking environments. Its Wireless Distribution System (WDS) feature allows for flexible extension of wireless coverage. It can be power via three alternative methods from either the Single LAN port for Power over Ethernet (PoE), DC jack providing the ability to back up each other with fail-over redundancy function, giving WAP-854NP reliable connectivity in mission critical situations.

WAP-854NP is easy-to-use and install with web-based administrative interface making configuration and client management simple and easy. In addition, management interfaces such as CLI and SNMP are also supported by WAP-854NP

WAP-854NP built-in software interface allows for communicating with other types of network management servers. WAP-854NP can further provide enhanced values in a well managed WLAN solution by our backend controlling gateway.

2.2 Specification

- Wireless Architecture Mode :
  - AP Mode
  - WDS Mode (Repeater/Brdige)

- Access Point Feature
  - Number of ESSID : 8
  - Number of associated clients per AP : 32
  - WDS Mode : to extend wireless coverage by connecting wirelessly to another WDS capable AP. Support up to 4 WDS links
  - Slot Time , ACK/CTS Timeout
  - RSSI threshold support
  - TX burst support
  - Beacon interval: adjustable to best adapt to the deployment environment
  - IAPP : to facilitable faster roaming for the stations among different APs nearby
  - RTS and fragmentation control
  - Adjustable transmission power : 7 Levels
  - Wireless site survey : for scanning the surrounding access points for connection
  - VLAN tag support

- Authentication/Encryption (Wireless Security)
  - Data encryption: WEP(64/128/152-bits) , WPA/WPA2 with TKIP or AES-CCMP
  - User Authentication : WEP, IEEE802.1X,WPA-PSK, WPA-Enterprise , MAC ACL
  - Setting for TKIP/CCMP/AES key's refreshing period
  - Support IEEE802.11 mixed mode, open and shared key authentication
  - Hidden ESSID: broadcast SSID option can be turn off to prevent SSID broadcast to the public
  - Station Isolation setting : when enabled , all stations associated with this AP can not communicate with each other
  - Support data encryption over WDS link

- Quality of Service
  - DiffServ/TOS
  - IEEE802.11p/COS
  - IEEE 802.11Q Tag VLAN priority control
  - IEEE802.11e WMM

- Management
  - ➔ Web-Based management interface
  - ➔ Remote configuration and management
  - ➔ Remote firmware upgradeable
  - ➔ Software one-button-click to reset back to factory defaults
  - ➔ Utilities for system configuration backup and restoration
  - ➔ SNMP MIBII support (v2c/v3)
  - ➔ NTP time synchronization
  - ➔ Syslog client
  - ➔ Support Event log
  - ➔ Support statistics on total transmission encountered and transmitting error occurred

WAP-854NP Hardware Specifications	
Base Platform	AR7240+AR9283
CPU Clock Speed	400 MHz
Wireless Radio	802.11bgn
Serial Port	1 (DB-9)
USB Port (Optional)	1 (ODM only)
Reset Switch Built-in	Push-button momentary contact switch
RF Channel Scan Hardware Button	Hardware Push-button to scan for a better channel to use
Standards Conformance	IEEE 802.3 / IEEE 802.3u
Ethernet Configuration	10/100BASE-TX auto-negotiation Ethernet port x 3 (RJ-45 connector) LAN * 3 Auto MDI/MDI-X enabled , IEEE802.3af Power Over Ethernet Compatible , Auto Fail over
SDRAM	On board : 32 Mbytes
Flash	On board : 8 Mbytes
Built-In LED Indicators	1x Power, 3 x LAN , 1x Status, 1x System

Wireless Specifications	
Network Standards Conformance	IEEE802.11 b /g /n compliant
Data Transfer Rate	IEEE802.11b：1 / 2 / 5.5 / 11Mbps (auto sensing) IEEE802.11g：6 / 9 / 12 / 18 / 24 / 36 / 48 / 54(auto sensing) IEEE802.11n : 300 (auto sensing)
Frequency Range	IEEE802.11b/g： 2.412 ~ 2.462GHz (USA) 2.412 ~ 2.484GHz (Japan) 2.412 ~ 2.472 GHz (Europe ETSI) 2.457 ~ 2.462 GHz (Spain) 2.457 ~ 2.472 GHz (France)
Media Access Protocol	CSMA / CA with ACK
Modulation Method	IEEE802.11b：DSSS (DBPK,DQPSK,CCK) IEEE802.11g/n：OFDM(64-QAM,16-QAM,QPSK,BPSK)
Operating Channels	802.11b/g/n : 11 for FCC,14 for Japan,13 for Europe, 2 for Spain, 4 for France
RF Output Power	100mW
Transmit Power Variation	802.11g/n : Up to 16 dBm 802.11b : up to 18 dBm
Frequency Response flatness	±1dB over operating range
Receiver Sensitivity	802.11b/g /n -90dBm@1Mbps, -86dBm@6Mbps,-84dBm@11Mbps,-69dBm@54Mbps
Environmental & Mechanical Characteristics	
Operating Temperature	-20 °C ~ 50 °C
Storage Temperature	-20 °C ~ 60 °C
Operating Humidity	10% to 80% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing
Antenna Connector	SMA-Type Connector
Power Supply	110 – 220V AC Power ; 12 VDC, 1.5A input. Support 802.3af Compliant , Power Over Ethernet (48V/0.3 A)
Unit Dimensions	205 x 125 x 35 (mm) (Width x Depth x Height)
Unit Weight	600g
Form Factor	Wall Mountable , Metal case compliant with IP50 standard
Certifications	FCC,CE, IP50,ROHS compliant

Chapter 3. Base Installations

3.1 Installations

3.1.1 System Requirements

- Standard 10/100Base T including five network cables with RJ-45 connectors
- All PCs need to install the TCP/IP network protocol

3.1.2 Panel Function Descriptions

Front Panel

1. **Power SOCKET (12V DC) :** Attach the power socket here.
2. **Reset :** Press the Reset button once to restart the system, The LED except Power indicator will be off before restarting.
3. **LAN1(POE)/LAN2/LAN3 :** Attach the Ethernet cable here for connecting to wired local network.
4. **Console :** The serial RS-232 DB9 cable attaches here.
5. **Scan Button :**
   - ➔ Press and hold the Reset button for **3** seconds and release to Scan New AP's Channel. The **STATUS** LED will be **FLASH**.
   - ➔ Press and hold the Reset button for more than **10** seconds to reset the system to default configurations. The **SYSTEM** LED will be **FLASH**.

Rear Panel

1. WAP-854NP supports 1 RF interface with 2 SMA connectors for Antenna connection.

LED Panel

1. **Power :** LED ON indicates power on, OFF indicates power off.
2. **LAN1/LAN2/LAN3 :** LED ON indicates connection, OFF indicates disconnection, FLASH indicates packets transmitting.
3. **WLAN :** LED ON indicates Wireless ready.
4. **SYSTEM :** LED ON indicates Flash busy, OFF indicates Flash Idle
5. **STATUS :** LED ON indicates System up, OFF indicates down, FLASH indicates Scan button activated.

3.1.3 Hardware Installation

Please follow the steps mentioned below to install the hardware of WAP-854NP

1. Place the WAP-854NP at a best location.

The best location for WAP-854NP is usually at the center of your wireless network.

2. Connect WAP-854NP to your outbound network device.

Connect one end of the Ethernet cable to the LAN port of WAP-854NP on the front panel and the other end of the cable to a switch, a router or a hub. WAP-854NP is then connected to your existing wired LAN network. The LAN LED indicator should be ON to indicate a proper connection.

3. There are two ways to supply power over to WAP-854NP

➔ Connect the DC power adapter to the WAP-854NP power socket on the front panel.

Please only use the power adapter supplied with the WAP-854NP package. Using a different power adapter may damage this system

➔ WAP-854NP is capable of transmitting DC current via its LAN1(PoE) port. Connect an IEEE 802.3af-compliant PSE device, e.g. A PoE Switch, to the LAN1(PoE) port of WAP-854NP with the Ethernet cable.

Now, the hardware installation is completed.

To double verify the wired connection between WAP-854NP and your switch/router/hub, please check the LED status indication of these network devices.

3.2 Software Configuration

3.2.1 Getting Start

WAP-854NP supports web-based configuration. Upon the completion of hardware installation, WAP-854NP can be configured through a PC by using its web browser such as Mozilla Firefox 3.5 or Internet Explorer version 8.0.

- Default IP Address : **192.168.2.254**
- Default IP Netmask : **255.255.255.0**
- Default User Name and Password : **root** / **default**

Step :

1. **IP Segment Set-up for Administrator's PC/NB**

Set the IP segment of the administrator's computer to be in the same range as WAP-854NP for accessing the system. Do not duplicate the IP Address used here with IP Address of WAP-854NP or any other device within the network

Example of Segment :

The value for underlined area can be changed as desired; the valid range is 1 ~ 254. However, 254 shall be avoided as it is already used by WAP-854NP; use 10 as an example here.

IP Address : 192.168.2.10

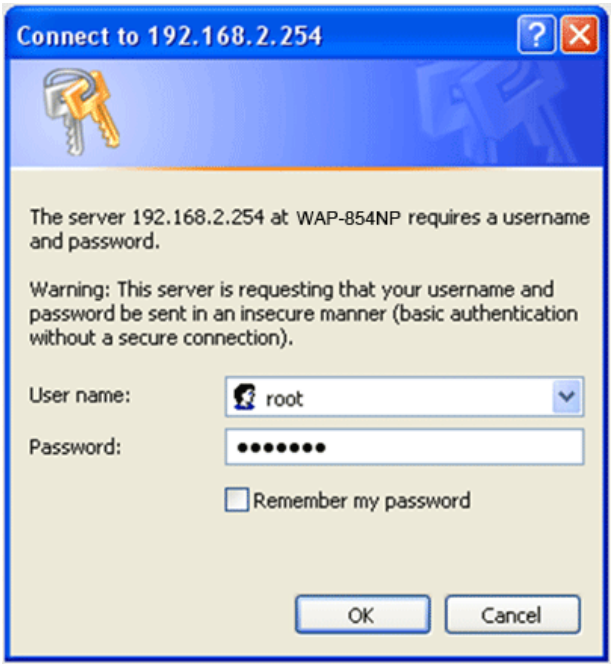
IP Netmask : 255.255.255.0

2. **Launch Web Browser**

Launch a web browser to access the web GUI of WAP-854NP by entering “http://192.168.2.254” in the address field.

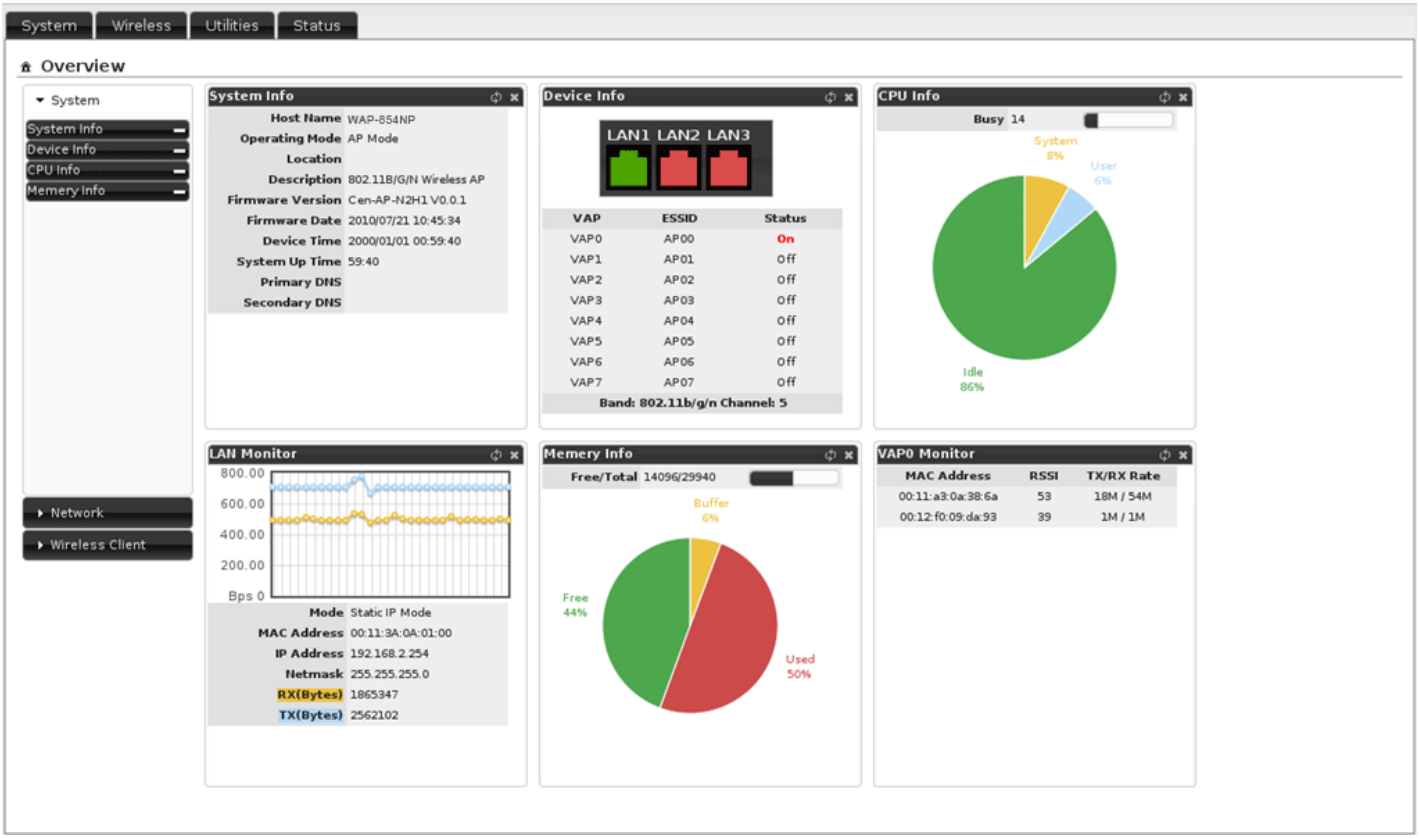
3. **System Login**

The following Administrator Login Page will appear. Enter “**root**” in the Username field, and “**default**” in the Password field


Connect to 192.168.2.254
The server 192.168.2.254 at WAP-854NP requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
root
Password:
Remember my password
OK
Cancel

4. Login Success

After a successful login, the "**System Overview**" will appear on the screen.



3.2.2 Quick Configuration

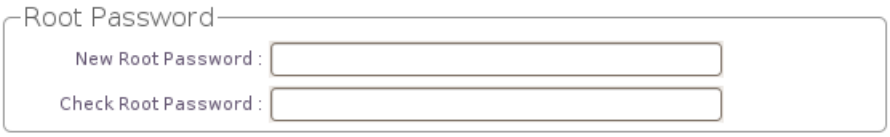
Configuration Steps :

Step 1 : Change Root's Password

➔ Click **System -> Management**, the Management Setup page will appear.

➔ Enter a ***New Root Password*** for the Root account ad retype in the ***Check Root Password*** field. (**4-30** alphanumeric and specific characters; **not** support **Space**)

➔ Click Save button.



For security concern, it is strongly recommended to change the Root password.

Step 2 : Configure Wireless General Settings

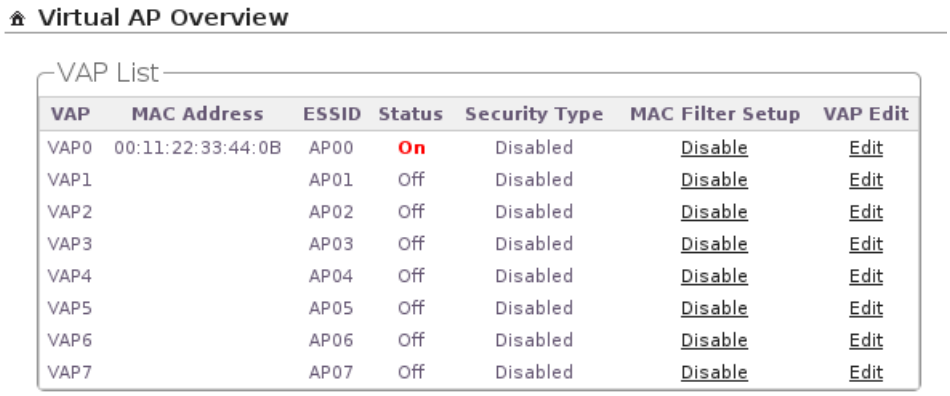
➔ Click **Wireless -> General Setup**, the Wireless General Setup page will appear.

➔ Select desired wireless **Band**, **Channel**.

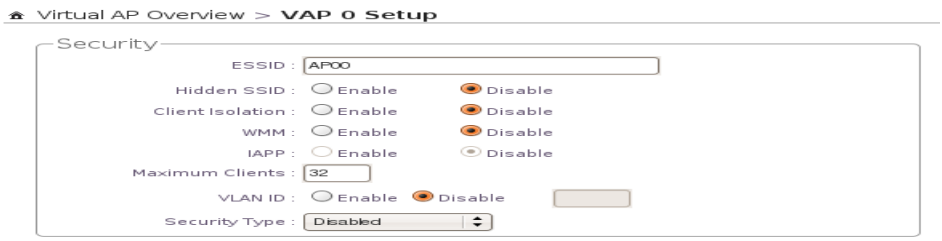
➔ Click ***Save*** button

Step 3 : Configure Virtual AP

➔ Click **Wireless -> Virtual AP Setup** ,the Virtual AP Overview page will appear.


Virtual AP Overview
VAP List
VAP MAC Address ESSID Status Security Type MAC Filter Setup VAP Edit
VAP0 00:11:22:33:44:0B AP00 On Disabled Disable Edit
VAP1 AP01 Off Disabled Disable Edit
VAP2 AP02 Off Disabled Disable Edit
VAP3 AP03 Off Disabled Disable Edit
VAP4 AP04 Off Disabled Disable Edit
VAP5 AP05 Off Disabled Disable Edit
VAP6 AP06 Off Disabled Disable Edit
VAP7 AP07 Off Disabled Disable Edit

➔ Click "**Edit**" button of VAP0's row on VAP List, the VAP0 Setup page will appear


Virtual AP Overview > VAP 0 Setup
Security
ESSID : AP00
Hidden SSID : Enable Disable
Client Isolation : Enable Disable
WMM : Enable Disable
IAPP : Enable Disable
Maximum Clients : 32
VLAN ID : Enable Disable
Security Type : Disabled

➔ Setup the broadcasting **ESSID** for easily identifying the system when device is trying to associate the service.

➔ Click ***Save*** button

On each configuration page, you may Click "**Save**" button to save the changes, but you must reboot the system upon the completion of all configuration settings for the changes to take effect. When clicking "**Save**", the following message will appear : "**Press Reboot to Enable New Setting.**"

Congratulation !

Now, WAP-854NP is installed and configured successfully.

Chapter 4. AP Mode Configuration

When AP mode is activated, the system can be configured as an Access Point. This section provides information in configuring the AP mode with graphical illustrations. WAP-854NP provides functions as stated below where they can be configured via a user-friendly web based interface.

OPTION	System	Wireless	Utilities	Status
Function	Operating Mode	General Setup	Profile Setting	Overview
	LAN	Advanced Setup	Firmware Upgrade	Extra Info
	Management	Virtual AP Setup	Network Utility	Event Log
	Time Server	Associated Clients	Reboot	
	SNMP	WDS Status		

Table 4-1: AP Mode Functions

After finishing the configuration of the settings, please click Save button and pay attention to see if a Reboot message appears on the screen. If such message appears, system must be restarted to allow the settings to take effect. All online users will be disconnected during restart.

WAP-854NP supports two operation modes; AP mode and WDS mode. Click **System -> Operating Mode**, the administrator can set the desired mode via this page, and then configure the system according to their deployment needs.

- ✓ **AP Mode :** Check ***AP Mode*** button to enable AP mode, and then click "**Save&Reboot**" to activate the setting.
- ✓ **WDS Mode** : Check **WDS *Mode*** button to enable AP mode, and then click "**Save&Reboot**" to activate the setting.

4.1 Connect WAP-854NP to the Wired Local Network

4.1.1 Network Requirement

Normally, WAP-854NP connects to a wired LAN and provides a wireless connection point to associate with wireless client as shown in Figure 4-1. Then, Wireless clients could access to LAN or Internet by associating themselves with WAP-854NP set in AP mode.

Figure 4-1 Access Point on a Wired LAN Configuration

4.1.2 Configure LAN Port

Here is instruction for how to setup the LAN. The connection types for LAN port : **Static IP** and **Dynamic IP**, Please click on **System -> LAN** and follow the below setting.

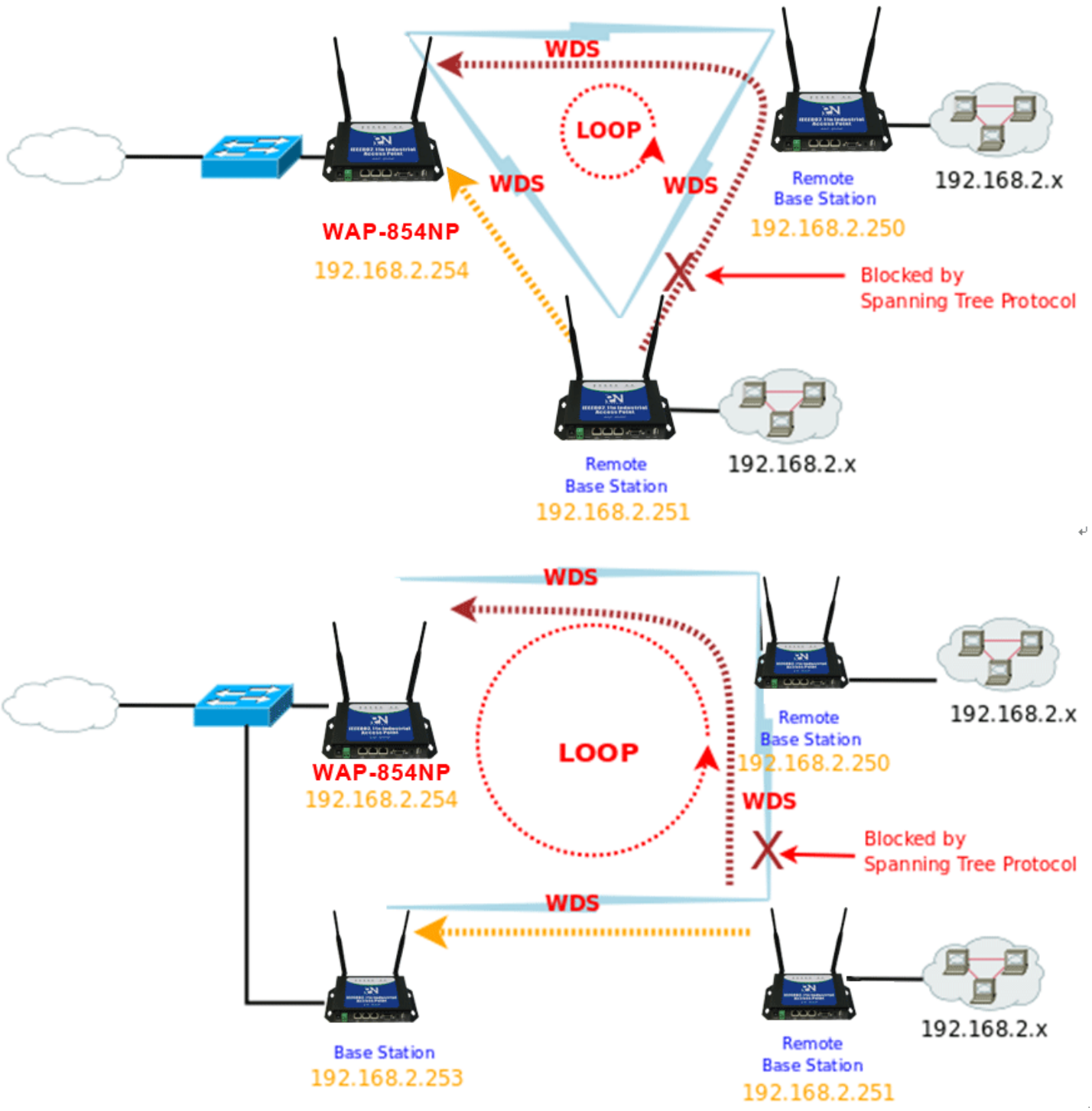
- **Mode :** Check either “Static IP” or “Dynamic IP” button as desired to set up the system IP of LAN port .
  - ➔ **Static IP :** The administrator can manually setup the LAN IP address when static IP is available/ preferred.
    - ✓ **IP Address :** The IP address of the LAN port; default IP address is 192.168.2.254
    - ✓ **IP Netmask :** The Subnet mask of the LAN port; default Netmask is 255.255.255.0
    - ✓ **IP Gateway :** The default gateway of the LAN port; default Gateway is 192.168.2.1
  - ➔ **Dynamic IP :** This configuration type is applicable when the WCB1200H5PX is connected to a network with the presence of a DHCP server; all related IP information will be provided by the DHCP server automatically.

    - ✓ **Hostname :** The Hostname of the LAN port

- **DNS :** Check either “No Default DNS Server” or “Specify DNS Server IP” button as desired to set up the system DNS.
  - **Primary :** The IP address of the primary DNS server.
  - **Secondary :** The IP address of the secondary DNS server.

- **802.1d Spanning Tree**

The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 4 WDS interfaces from WDS0 to WDS3. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d. The Spanning tree always enabled on WAP-854NP. Below Figures depict a loop for a bridged LAN between LAN and WDS link



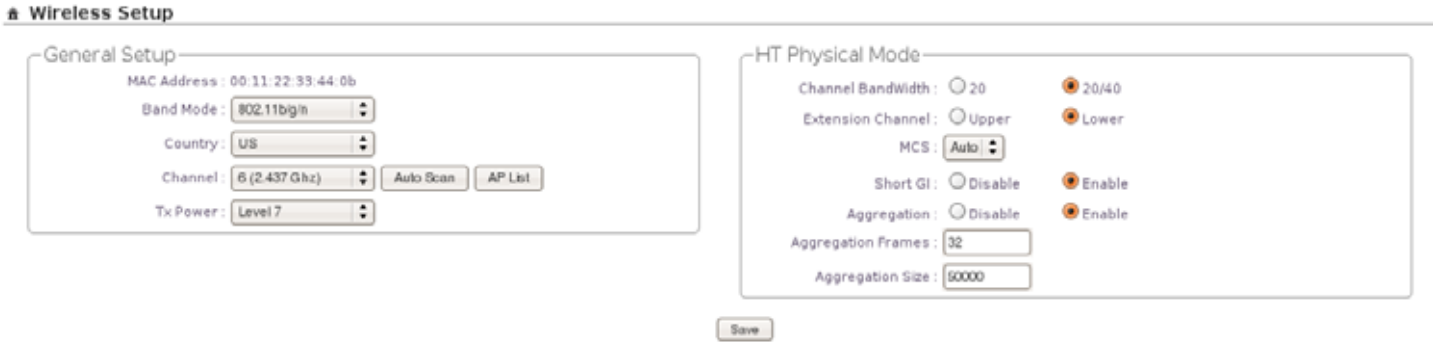
Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

4.2 Create Your Wireless Network

The system manager can configure related wireless settings, **General Settings, Advanced Settings, Virtual AP(VAP) Setting, Security Settings** and **Access Control Settings**.

4.2.1 Configure Wireless General Setup

The administrator can change the data transmission, channel and output power settings for the system. Please click on **Wireless -> General Setup** and follow the below setting.



- **MAC address :** The MAC address of the Wireless interface is displayed here.
- **Band Mode :** Select an appropriate wireless band; bands available are 801.11b, 802.11b/g, 802.11b/g/n and 802.11n.
- **Transmit Rate Control :** Select the desired rate from the drop-down list; the options are auto or ranging from 1Mbps to 54Mbps for 802.11b/g modes, or 1Mbps to 11Mbps for 802.11b mode.
- **Country :** Select the desired country code from the drop-down list; the options are US, ETSI and Japan.
- **Channel :** The channel range will be changed by selecting different country code. The channel range from **1** to **11** for **US** country code, or **1** to **13** for **ETSI** country code, or **1** to **14** for Japan(Channel **14** only for **802.11b** Rate).

Click “**Auto Scan**”, the channel will change to next channel. Click “**AP List**” button, the system will show current all AP list.

AP Site Survey List

ESSID	MAC Address	Channel	Signal Level	Security Type
AP00	00:11:22:33:44:03	6	-1 dBm	None
MENTHOLATUM	00:11:22:5A:5B:5E	11	-1 dBm	WEP
MENTHOLATUM2	06:11:22:5A:5B:5E	11	-1 dBm	WEP
				Current Frequency:2.437 GHz (Channel 6)

Rescan Close

- **Tx Power :** You can adjust the output power of the system to get the appropriate coverage for your wireless network. Select LEVEL 1 to LEVEL 7 needed for your environment. If you are not sure of which setting to choose, then keep the default setting, **LEVEL 7**.

When **Band Mode** select in **802.11b/gn or 802.11n**, the **HT Physical Mode** settings should be show immediately.

- **Channel Bandwidth :** The "**20/40**" MHz option is usually best. The other option is available for special circumstances.
- **Extension Channel :** Only for Channel Bandwidth "**40**" MHz. Select the desired channel bonding for control.
- **MCS :** This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
- **Shout GI :** Short Guard Interval, by default, it's "Enable". it's can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **Aggregation :** By default, it's "Enable". To "Disable" to deactivated Aggregation.

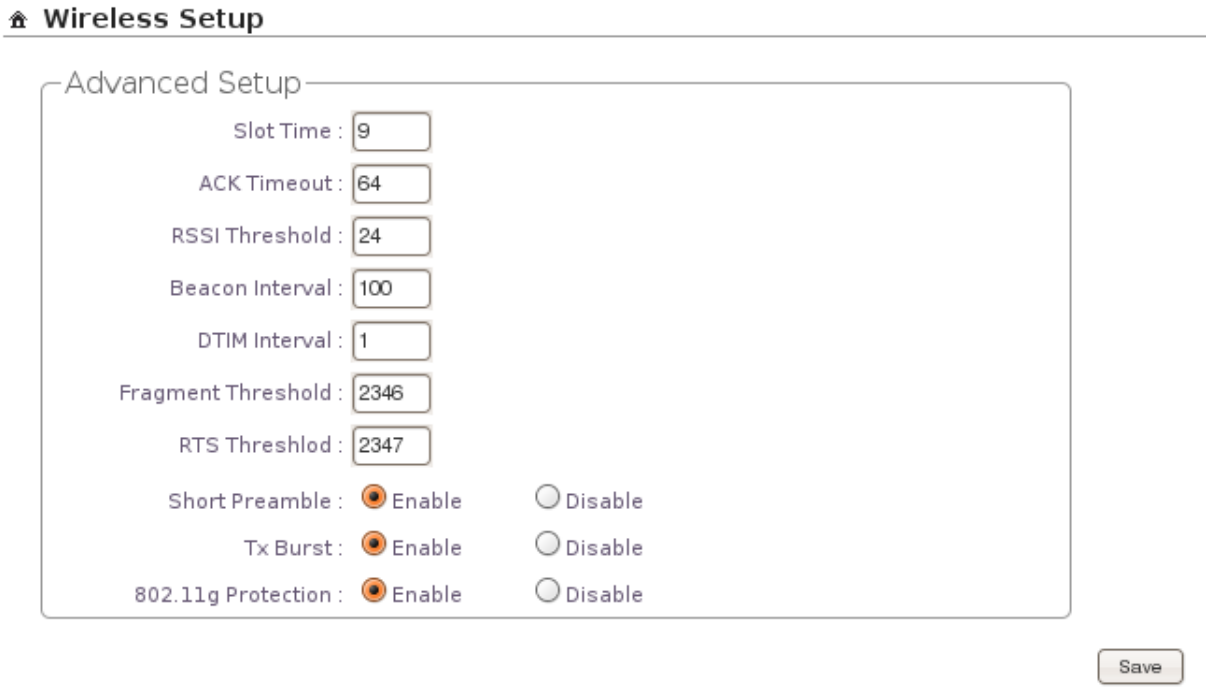
A part of the 802.11n standard (or draft-standard). It allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header.

- Aggregation Frames : The Aggregation Frames is in the range of **2~64**, default is **32**. It determines the number of frames combined on the new larger frame.
- Aggregation Size : The Aggregation Size is in the range of **1024~65535**, default is **50000**. It determines the size (in Bytes) of the larger frame.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes. The items in this page is for AP's RF general settings and will be applied to **all VAPs and WDS Link**.

4.2.2 Configure Wireless Advanced Setup

The administrator can change the Slot Time, ACK Timeout, RTS threshold and fragmentation threshold settings for the system. Please click on **Wireless -> Advanced Setup** and follow the below setting.



- **Slot Time :** Slot time is in the range of **9~1489** and set in unit of ***microsecond***. The default value is **9** microsecond.

  Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. For a sender and receiver own right of the channel the shorter slot time help manage shorter wait time to re-transmit from collision because of hidden wireless clients or other causes. When collision sources can be removed sooner and other senders attempting to send are listening the channel(CSMA/CA) the owner of the channel should continue ownership and finish their transmission and release the channel. Then, following ownership of the channel will be sooner for the new pair due to shorter slot time. However, when long duration of existing collision sources and shorter slot time exist the owners might experience subsequent collisions. When adjustment to longer slot time can't improve performance then RTS/CTS could supplement and help improve performance.

- **ACK Timeout :** ACK timeout is in the range of **1~372** and set in unit of ***microsecond***. The default value is **64** microsecond.

  All data transmission in 802.11b/g request an "Acknowledgement" (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as "ACK Timeout".

ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to “Resend” packet before ACK is received, and throughput become low due to excessively high re-transmission.

ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor performance the ACK Timeout could be made longer to accommodate.

Slot Time and ACK Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

- **RSSI Threshold :** RSSI(Received Signal Strength Indication) Threshold is in the range of **-127 ~ 128**. The default value is **24**. RSSI Threshold can be used to control the level of noise received by the device.
- **Beacon Interval :** Beacon Interval is in the range of **40**~**3500** and set in unit of *millisecond*. The default value is **100** msec.

  Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called “Beacon”. Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate.

  All the radio stations received beacon recognizes the existence of such AP, and may proceed next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.

  By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.
- **DTIM Interval :** The DTIM interval is in the range of **1**~**255**. The default is **1**.

  DTIM is defined as *Delivery Traffic Indication Message*. It is used to notify the wireless stations, which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.

  A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.

- **Fragment Threshold :** The Fragment Threshold is in the range of **256**~**2346** byte. The default is **2346** byte.

  Each Wi-Fi packet can be divided into smaller packets, marked with a sequential fragment number and re-assemble in the receiving ends. The purpose is to make a short frame, instead of long frame, transmitting by radio in a heavy noisy environment. Because of sending smaller frames, corruptions are much less likely to occur. The pros is obvious, the cons is the overhead for transmission. So, in a clean environment, higher fragment threshold can be an option to increase throughput.

  Fragmentation will be triggered by setting the Fragment Threshold, usually in Byte-length. Only when the frame size is over the Threshold, fragmentation will take place automatically.

- **RTS Threshold :** TRTS Threshold is in the range of **1~2347** byte. The default is **2347** byte.

  The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.

- **Short Preamble :** By default, it's "***Enable***". To ***Disable*** is to use Long 128-bit Preamble Synchronization field.

  The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.

- **Tx Burst :** By default, it's "***Enable***". To ***Disable*** is to deactivate Tx Burst.

With TX burst enabled, AP will send many packets in a burst, without collision detection and RTS/CTS for each packet. TX Burst have better throughput but cause interference with other APs in channel.

- **802.11g Protection :** Click ***Enable*** button to activate 802.11g Protection Mode, and Disable to inactivate 802.11g Protection Mode.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes. The items in this page is for AP's RF general settings and will be applied to **all VAPs and WDS Link**.

4.2.3 Create Virtual AP

The WAP-854NP support broadcasting multiple SSIDs, allowing the creation of Virtual Access Points, partitioning a single physical access point into **8** logical access points, each of which can have a different set of security, VLAN Tag(ID) and network settings. If wireless client connect to wired area network with VLAN Tag(ID), the administrator can use dump switch or VLAN switch on wired area network, a **Figure 4-2** shows multiple SSIDs with different VLAN settings use dump switch connect to wired area. a **Figure 4-3** shows multiple SSIDs with different VLAN settings use VLAN switch connect to wired area.

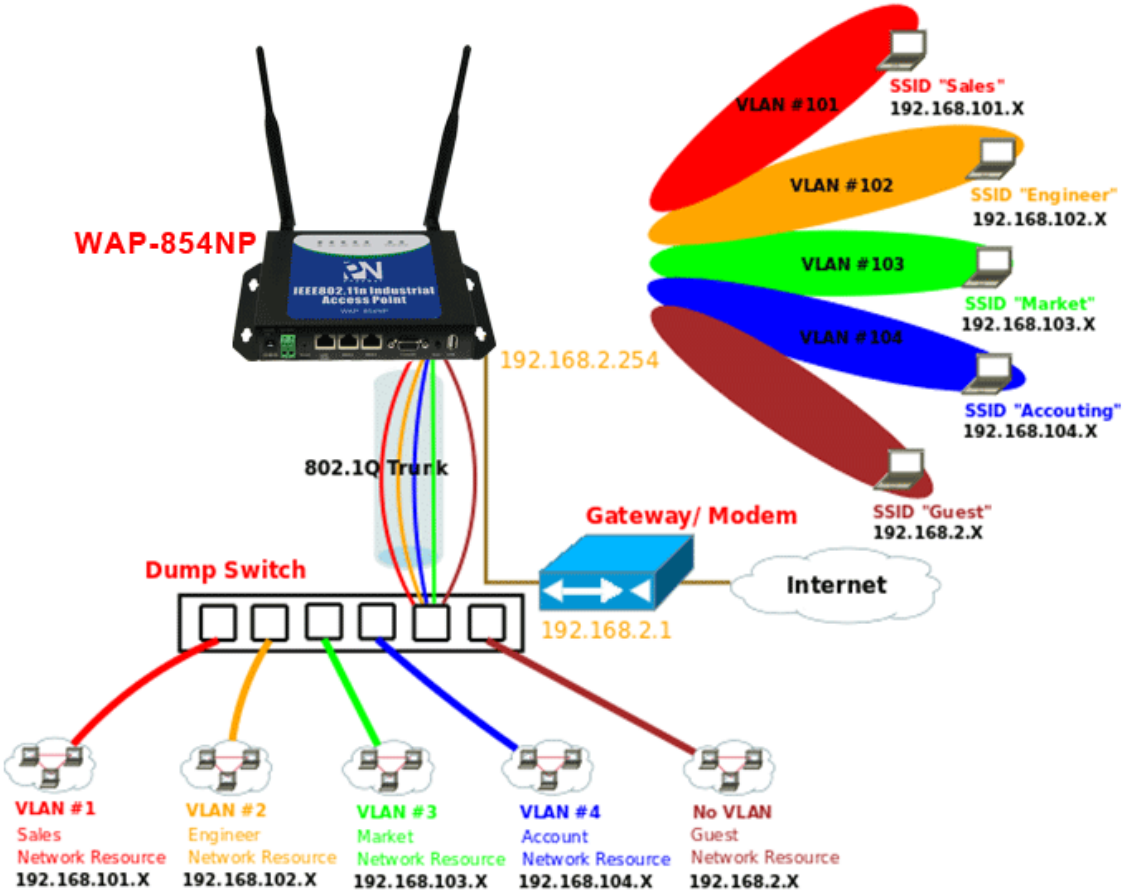


Figure 4-2 Multiple SSIDs with different VLAN settings use dump switch connect to wired area.

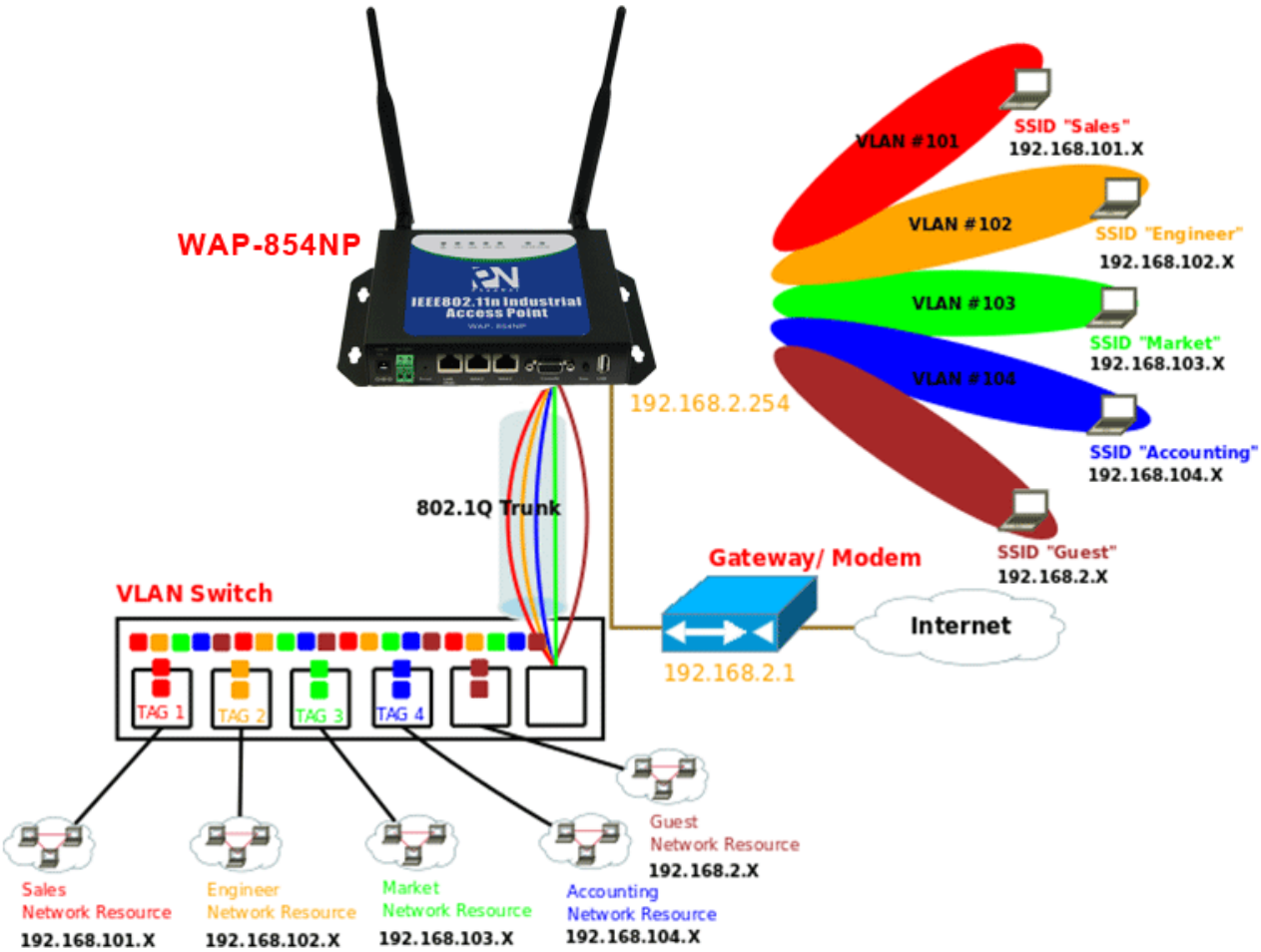
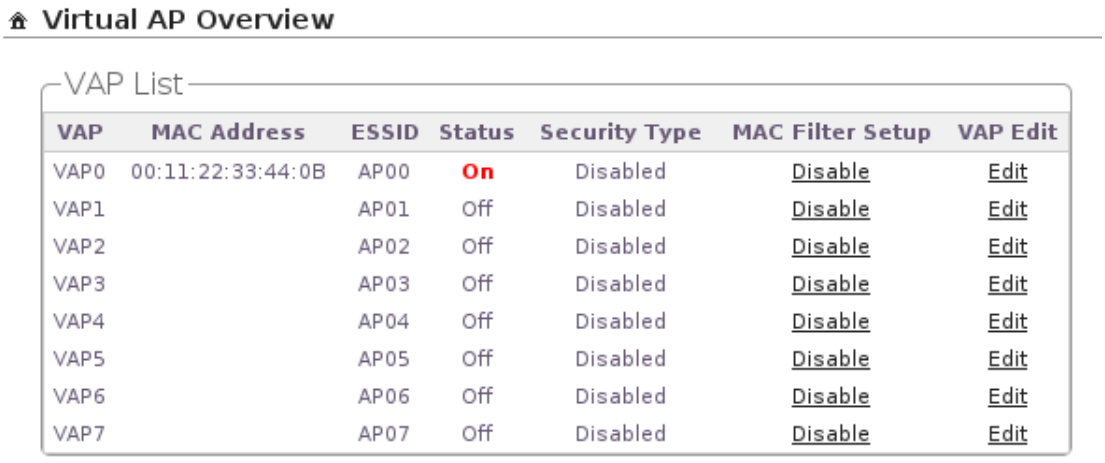


Figure 4-3 Multiple SSIDs with different VLAN settings use VLAN switch connect to wired area.

The administrator can create Virtual AP via this page. Please click on **Wireless -> Virtual AP Setup** and follow the below setting.

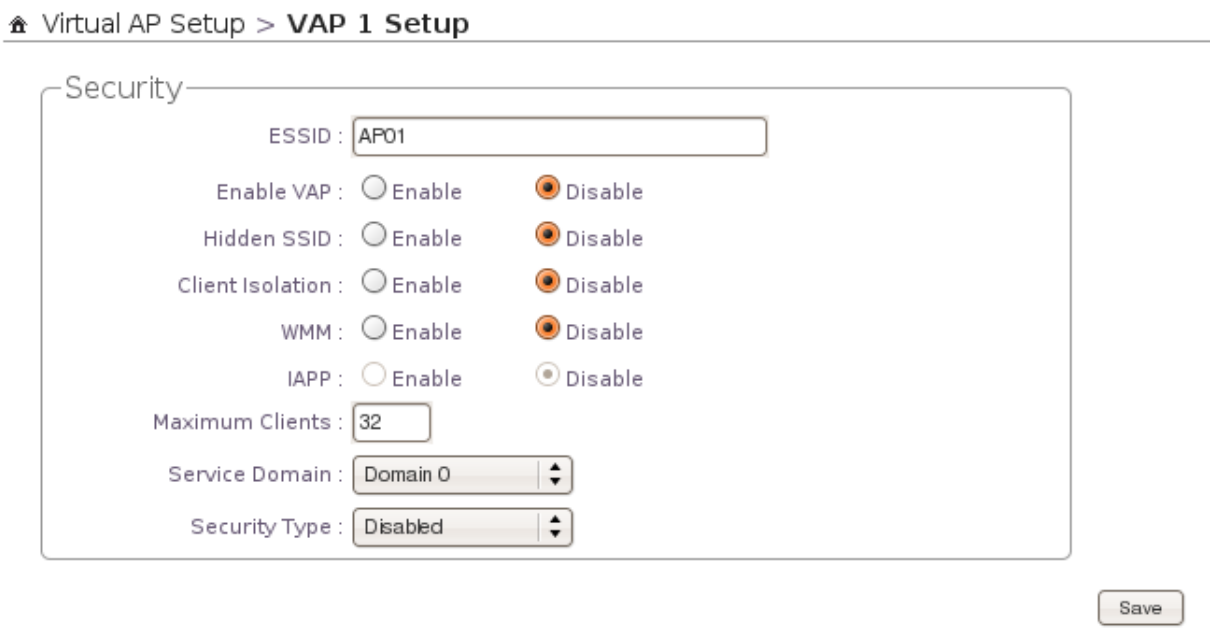

Virtual AP Overview
VAP List
VAP MAC Address ESSID Status Security Type MAC Filter Setup VAP Edit
VAP0 00:11:22:33:44:0B AP00 On Disabled Disable Edit
VAP1 AP01 Off Disabled Disable Edit
VAP2 AP02 Off Disabled Disable Edit
VAP3 AP03 Off Disabled Disable Edit
VAP4 AP04 Off Disabled Disable Edit
VAP5 AP05 Off Disabled Disable Edit
VAP6 AP06 Off Disabled Disable Edit
VAP7 AP07 Off Disabled Disable Edit

- **VAP :** Indicate the system's Virtual AP.
- **MAC Address :** The MAC address of the VAP Interface is displayed here. When you enable AP and reboot system, the MAC address will display here.
- **ESSID :** Indicate the ESSID of the respective Virtual AP
- **Status :** Indicate the current Status of the respective Virtual AP. The **VAP0** always on.
- **Security Type :** Indicate an used security type of the respective Virtual AP.
- **MAC Filter :** Indicate an used MAC filter of the respective Virtual AP. Click button to configure MAC Filter of the respective Virtual AP.
- **Edit :** Click **Edit** button to configure Virtual AP's settings.

4.2.3.1 Configure Virtual AP

For each Virtual AP, administrators can configure general settings and security type.

Click **Wireless -> Virtual AP**, click "**Edit**" of Virtual AP List and then Virtual AP Configuration page appears.


Virtual AP Setup > VAP 1 Setup
Security
ESSID : AP01
Enable VAP : Enable Disable
Hidden SSID : Enable Disable
Client Isolation : Enable Disable
WMM : Enable Disable
IAPP : Enable Disable
Maximum Clients : 32
Service Domain : Domain 0
Security Type : Disabled
Save

- **ESSID :** Extended Service Set ID indicates the SSID which the clients used to connect to the VAP. ESSID will determine the service type of a client which is assigned to the specified VAP.
- **Enable AP :** By default, it's "***Disable***" for VAP1 ~ VAP6. **The VAP0 always enabled**.

Select "***Enable***" to activate VAP or click "***Disable***" to deactivate this function

- **Hidden SSID :** Select this option to enable the SSID to broadcast in your network. When configuring the network, it is suggested to enable this function but disable it when the configuration is complete. With this enabled, someone could easily obtain the SSID information with the site survey software and get unauthorized access to a private network. With this disabled, network security is enhanced and can prevent the SSID from begin seen on networked.
- **Client Isolation :** Select **Enable**, all clients will be isolated from each other, that means all clients can not reach to other clients.

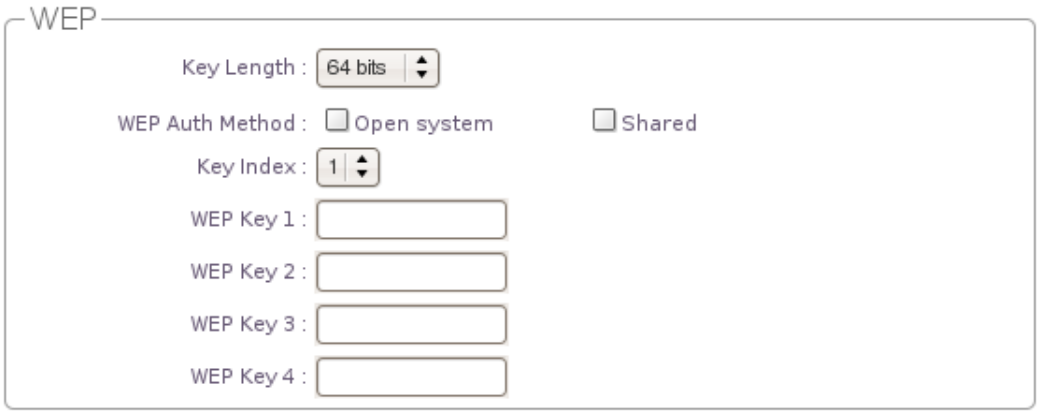
- **WMM :** Select Enable, the packets with QoS WMM will has higher priority.
- **IAPP Support :** Inter Access-Point Protocol is designed for the enforcement of unique association throughout a ESS(Extended Service Set) and for secure exchange of station's security context between current access point (AP) and new AP during hand off period.

IAPP only used on WPA-PSK and WPA2-PSK security type. Only one of VAPs can be enabled

- **Maximum Clients :** Enter maximum number of clients to a desired number. For example, while the number of client is set to 32, only 32 clients are allowed to connect with this VAP.
- **Service Domain :** Select the desired Service Domain from the drop-down list.
- **Security Type :** Select the desired security type from the drop-down list; the options are WEP, WPA-PSK, WPA2-PSK, WPA-Enterprise, WPA2-Enterprise and WEP 802.1X.

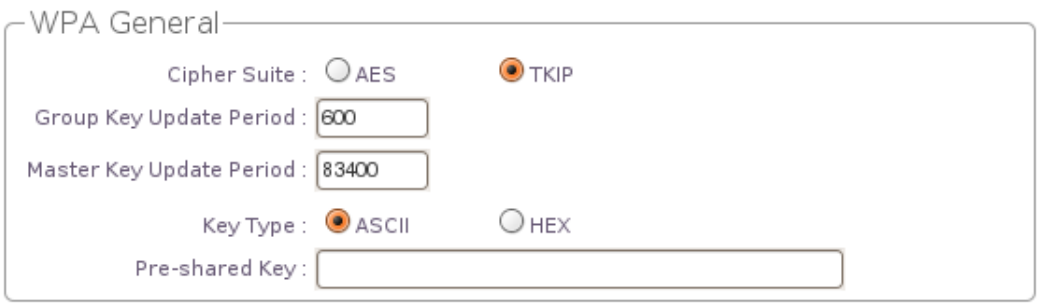
➔ **Disable :** Data are unencrypted during transmission when this option is selected.

➔ **WEP :** WEP, Wired Equivalent Privacy, is a data encryption mechanism based on a 64-bit, 128-bit or 152-bit shared key. Select ***WEP*** as the security type from the drop down list as desired.



- ✓ **Key Length :** Select the desire option are ***64 bits***, ***128 bits*** or ***152 bits*** from drop-down list.
- ✓ **WEP auth Method :** Enable the desire option among ***Open system*** or ***Shared***.
- ✓ **Key Index :** Select key index used to designate the WEP key during data transmission. 4 different WEP keys can be configured at the same time, but only one is used. Effective key is set with a choice of WEP Key 1, 2, 3, or 4.
- ✓ **WEP Key :** Enter HEX format WEP key value; the system support up to 4 sets of WEP keys.

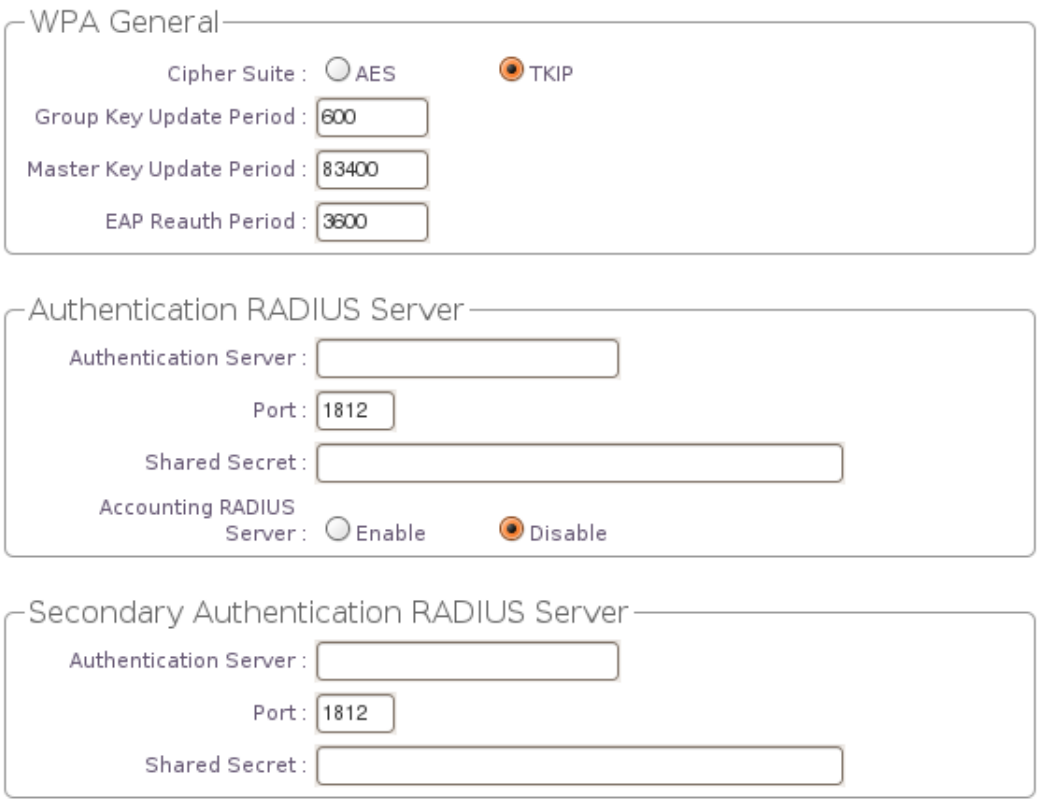
➔ **WPA-PSK (or WPA2-PSK) :** WPA (or WPA2) Algorithms, allows the system accessing the network by using the WPA-PSK (WPA2-PSK) protected access.



- ✓ **Cipher Suite :** Check on the respected button to enable either **AES** or **TKIP** cipher suites; default is **TKIP**.
- ✓ **Group Key Update Period :** This time interval for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is **600** seconds.
- ✓ **Master Key Update Period :** This time interval for re-keying GMK (master key used internally to generate GTKs) in seconds. Enter the time-length required; the default time is **83400** seconds.
- ✓ **Key Type :** Check on the respected button to enable either **ASCII** or **HEX** format for the Pre-shared Key.
- ✓ **Pre-shared Key :** Enter the information for pre-shared key; the format of the information shall according to the key type selected.

Pre-shared key can be either entered as a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.

➔ **WPA-Enterprise (or WPA2-Enterprise):** The RADIUS authentication and encryption will be both enabled if this selected. The WAP-854NP support two 802.1x Authentication/ Accounting Radius Server



✓ **WPA General Settings :**

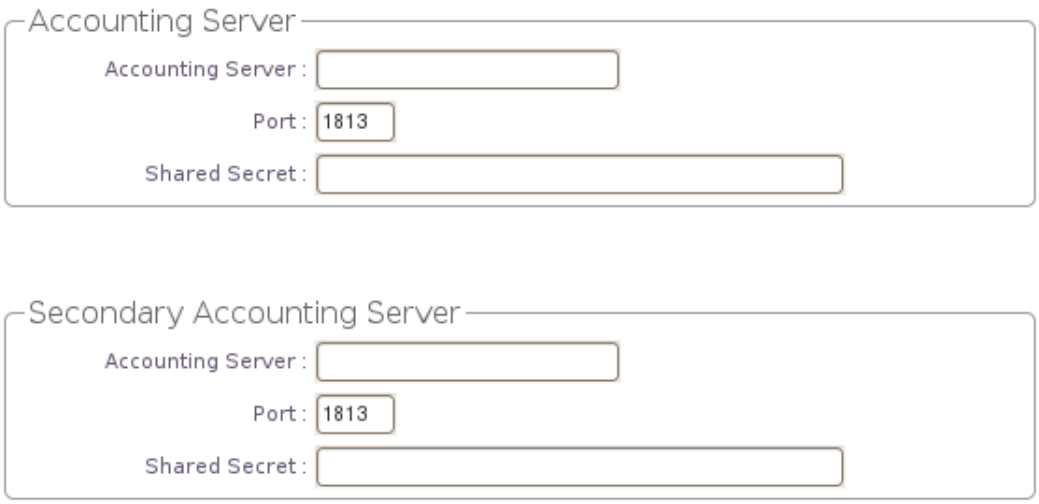
- **Cipher Suite :** Check on the respected button to enable either **AES** or **TKIP** cipher suites.
- **Group Key Update Period :** This time interval for re-keying GTK (broadcast/ multicast encryption keys) in seconds. Enter the time-length required; the default time is **600** seconds.
- **Master Key Update Period :** This time interval for re-keying GMK (master key used internally to generate GTKs) in seconds. Enter the time-length required; the default time is **83400** seconds.
- **EAP Reauth Period :** EAP re-authentication period in seconds; default is **3600**; **0** indicates **disable** re-authentication.

✓ **Authentication RADIUS Server Settings :**

- **Authentication Server :** Enter the IP address of the Authentication RADIUS server.
- **Port :** The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.

- **Shared secret :** The secret key for system to communicate with Authentication RADIUS server. Support 1 to 64 characters.
- **Accounting RADIUS Server :** Check on the respected button to enable either Enable or Disable accounting RADIUS server.

✓ **Accounting Server Settings :**

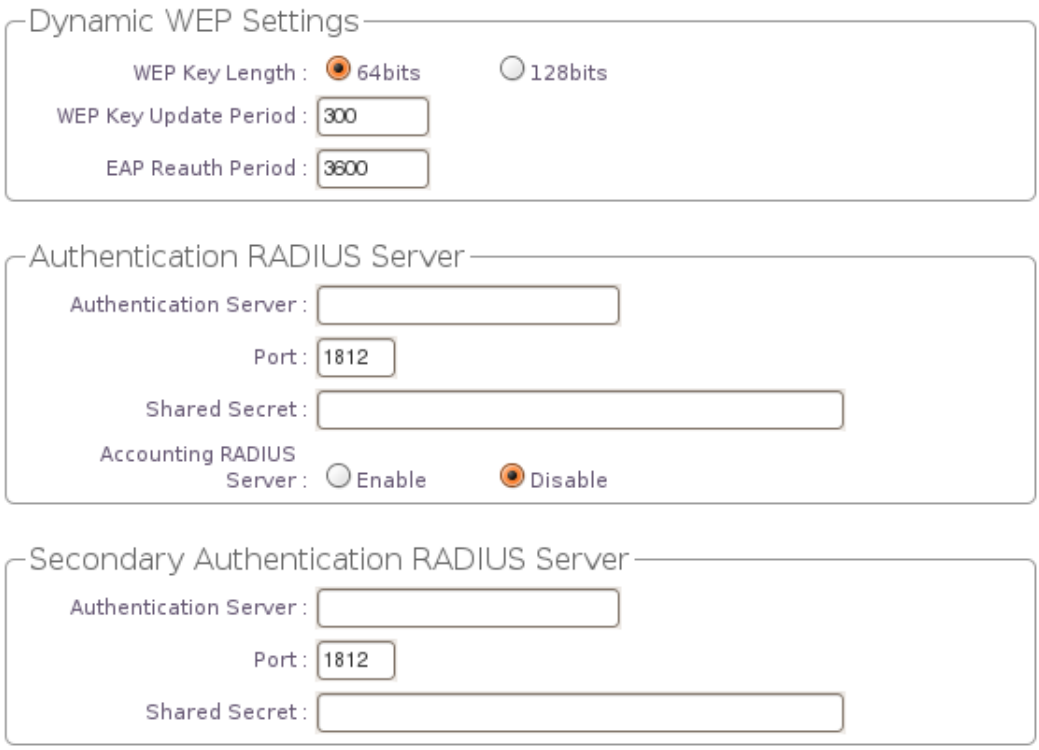


- **Accounting Server :** Enter the IP address of the Accounting RADIUS server.
- **Port :** The port number used by Accounting RADIUS server. Use the default 1813 or enter port number specified.
- **Shared Secret :** The secret key for system to communicate with Accounting RADIUS server. Support 1 to 64 characters.

➔ **WEP 802.1X :** When WEP 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete the configuration.

✓ **Dynamic WEP Settings :**

- **WEP Key length :** Check on the respected button to enable either 64bits or 128bits key length. The system will automatically generate WEP keys for encryption.
- **WEP Key Update Period :** The time interval WEP will then be updated; the unit is in seconds; default is **300** seconds; **0** indicates no re-key.
- **EAP Reauth Period :** EAP re-authentication period in seconds; default is **3600**; **0** indicates **disable** re-authentication.



✓ **Authentication RADIUS Server Settings :**

- **Authentication Server :** Enter the IP address of the Authentication RADIUS server.
- **Port :** The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.
- **Shared Secret :** The secret key for system to communicate with Accounting RADIUS server. Support 1 to 64 characters.
- **Accounting RADIUS Server :** Check on the respected button to enable either Enable or Disable accounting RADIUS server.

✓ **Accounting Server Settings :**

- **Accounting Server :** Enter the IP address of the Accounting RADIUS server.
- **Port :** The port number used by Accounting RADIUS server. Use the default 1813 or enter port number specified.
- **Shared Secret :** The secret key for system to communicate with Accounting RADIUS server. Support 1 to 64 characters.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

4.2.3.2 Block Wireless Clients

In this function, the administrator can be allow or reject clients to access Virtual AP. Please click on **Wireless -> Virtual AP Setup**, then click button on column of MAC Filter Setup. The MAC Filter Configuration page appears. Follow the below setting.

- **Action :** Select the desired access control type from the drop-down list; the options are "**Disabled**", "**Only Deny List MAC**" or "**Only Allow List MAC**".

  define certain wireless clients in the list which will have denied access to the Access Point while the access will be granted for all the remaining clients – **Action** is set to **Only Deny List MAC**.

  define certain wireless clients in the list which will have granted access to the Access Point while the access will be denied for all the remaining clients – **Action** is set to **Only Allow List MAC**.

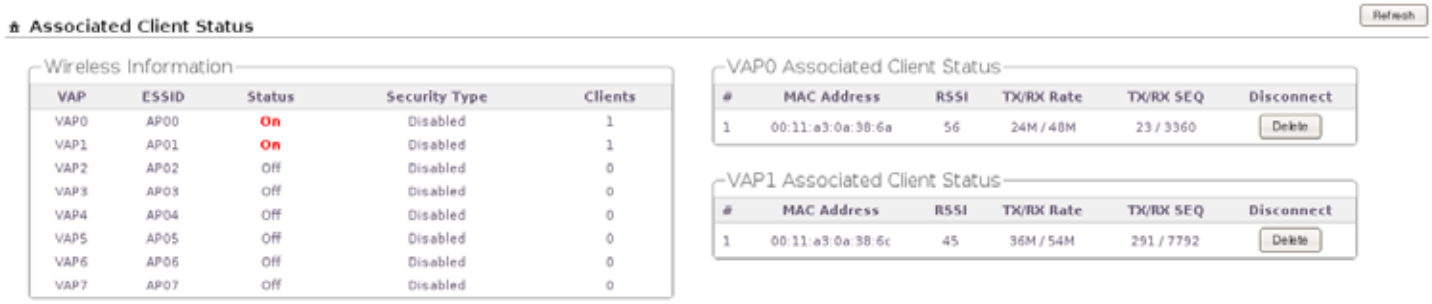
- **MAC Address :** Enter MAC address in this field. There are maximum **20** clients users allowed in this MAC address list.

The MAC Address of the wireless clients can be added and removed to the MAC Filter List using the "**Add**" and "**Delete**" buttons. Click ***Reboot*** button to activate your changes

MAC Access Control is the weakest security approach. WPA or WPA2 security methods should be used when possible.

4.2.3.3 Monitor Associated Wireless Clients

The administrator can obtain detailed wireless information and all associated clients status via this page. Please click on Wireless -> Associated Clients. The the Associated Clients Status appears.


Associated Client Status
Refresh
Wireless Information
VAP ESSID Status Security Type Clients
VAP0 AP00 On Disabled 1
VAP1 AP01 On Disabled 1
VAP2 AP02 Off Disabled 0
VAP3 AP03 Off Disabled 0
VAP4 AP04 Off Disabled 0
VAP5 AP05 Off Disabled 0
VAP6 AP06 Off Disabled 0
VAP7 AP07 Off Disabled 0
VAP0 Associated Client Status
MAC Address RSSI TX/RX Rate TX/RX SEQ Disconnect
1 00:11:a3:0a:38:6a 56 24M / 48M 23 / 3360 Delete
VAP1 Associated Client Status
MAC Address RSSI TX/RX Rate TX/RX SEQ Disconnect
1 00:11:a3:0a:38:6c 45 36M / 54M 291 / 7792 Delete

- **Wireless Information :** Display the Virtual AP configuration information of the system.
  - ➔ **VAP :** Display number of system's Virtual AP.
  - ➔ **ESSID :** Extended Service Set ID of the Virtual AP.
  - ➔ **Status :** Display Virtual AP status currently.
  - ➔ **Security Type :** Security type activated by the Virtual AP.
  - ➔ **Clients :** Number of clients currently associated to the Virtual AP.

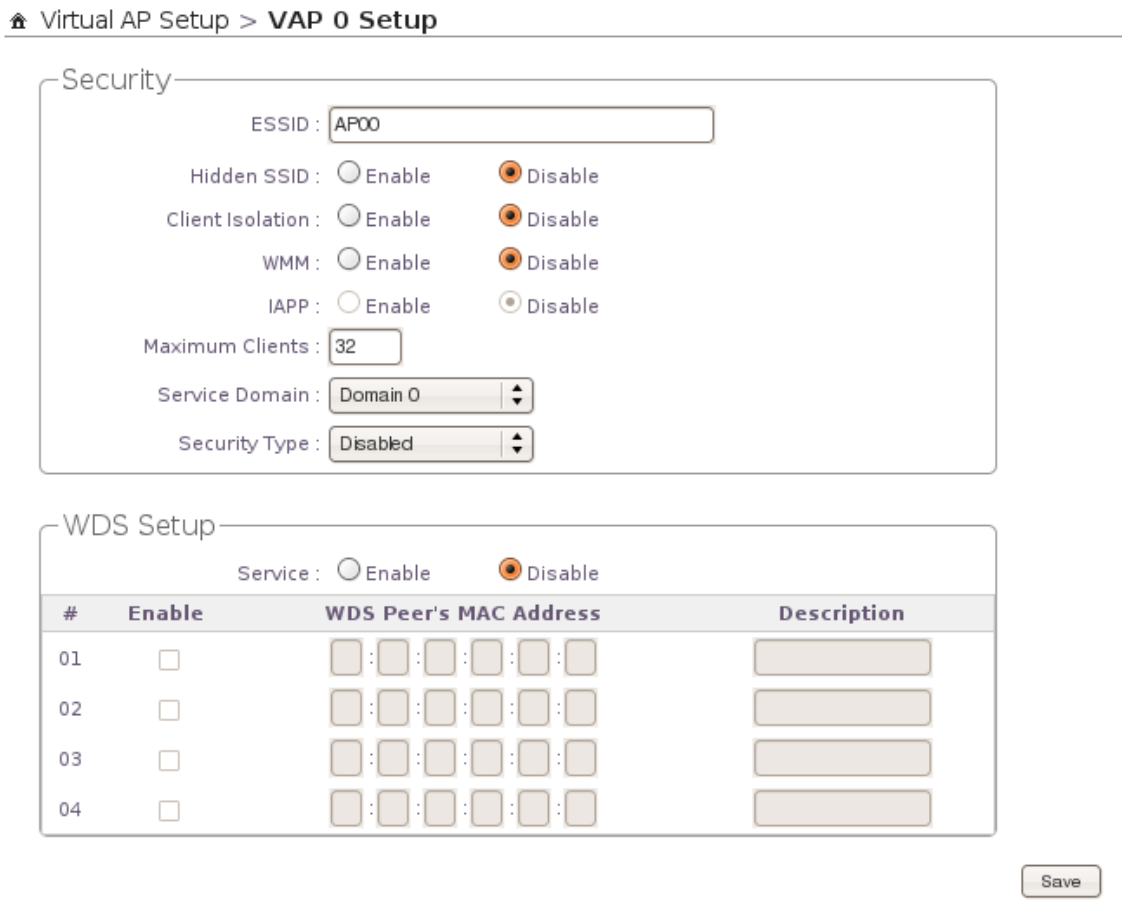
- **Associated Client Status :** Display the Virtual AP configuration information of the system.
  - ➔ **AP :** Virtual AP which the device is associated with.
  - ➔ **RSSI :** Indicate the RSSI of the respective client's association.
  - ➔ **TX/RX Rate :** Indicate the TX/RX Rate of the respective client's association.
  - ➔ **TX/RX SEQ :** Indicate the TX/RX sequence of the respective client's association.
  - ➔ **Disconnect :** Administrator can kick out a specific client, click “**Delete**” button to kick out specific client

4.3 Expand Your Wireless Network

4.3.1 Create WDS Link

The administrator can create WDS Links for expanding wireless network via this page.

Please click on **Wireless -> Virtual AP Setup -> VAP0 Setup** and follow the below setting.



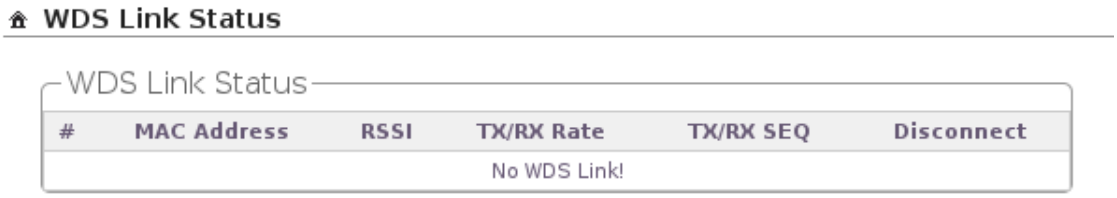
- **Service :** By default, it's “Disable”. To “Enable” to activate WDS.
- **Enable :** Click ***Enable*** checkbox to create WDS link.
- **WDS Peer's MAC Address :** Enter the MAC address of WDS peer.
- **Description :** Description of WDS link.
- **WMM :** Select Enable, the packets with QoS WMM has higher priority.

If WDS activate, the Security Type only support “**WEP**” on VAP0

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes.

4.3.2 View WDS Link Status

Peers MAC Address, antenna 0/1 received signal strength, phy mode and channel bandwidth for each WDS are available.



- **MAC Address :** Display MAC address of WDS peer.
- **RSSI :** Indicate the RSSI of the respective WDS's link.
- **TX/RX Rate :** Indicate the TX/RX Rate of the respective WDS's link.
- **TX/RX SEQ :** Indicate the TX/RX sequence of the respective WDS's link.
- **Disconnect :** Administrator can kick out a specific client, click “**Delete**” button to kick out specific WDS's link

4.4 Manage the System

4.4.1 Configure System Time

System time can be configured via this page where manual setting and NTP server configuration are both supported. Please click on **System -> Time Server** and follow the below setting.

- **Local Time :** Display the current time of the system.
- **Setup Time Use NTP :** Enable Network Time Protocol, NTP, to synchronize the system time with NTP server.
  - ➔ **Default NTP Server :** Select the NTP Server from the drop-down list.
  - ➔ **Time Zone :** Please set a time zone from where the accurate time can be supplied, **(GMT+08:00) Taipei** for example.
  - ➔ **Daylight saving time :** Enable Daylight saving time from where the accurate time needed.

If Time server setting selected in “Setup Time User NTP”, please verify system's DNS and Default Gateway setting first.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

4.4.2 Configure Management

The administrator can later obtain the geographical location of the system via the information configured here. The administrator also can change system password and configure system login methods. Please click **System -> Management** and follow the below settings.

- **System Information**
  - ➔ **System Name :** Enter a desired name or use the default provided.
  - ➔ **Description :** Denote further information of the system.
  - ➔ **Location :** Enter related geographical location information of the system; administrator/manager will be able to locate the system easily.

- **Root Password :** Log in as a root user and is allowed to change its own. Root user also can change **admin** user's and **operator** user's password. Click ***Save*** button to activate the new password.
  - ➔ **New Password :** Please input the new password of administrator.
  - ➔ **Check New Password :** Please input again the new password of administrator.

- **Admin Login Methods :** The admin manager can enable or disable system login methods, it also can change services port. Click ***Save*** button to activate the admin login methods.
  - ➔ **Enable HTTP :** Select Enable HTTP to activate HTTP Service
  - ➔ **HTTP Port :** Please input 1 ~ 65535 value to set HTTP Port; default value is **80**
  - ➔ **Enable Telnet :** Select Enable HTTP to activate HTTP Service
  - ➔ **Telnet Port :** Please input 1 ~ 65535 value to set HTTP Port; default value is **23**

- **Ping Watchdog :** The ping watchdog sets the WAP-854NP Device to continuously ping a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, the WAP-854NP device will automatically reboot. This option creates a kind of "fail-proof" mechanism.

Ping Watchdog is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. The Ping works by sending ICMP “echo request” packets to the target host and listening for ICMP “echo response” replies. If the defined number of replies is not received, the tool reboots the device.

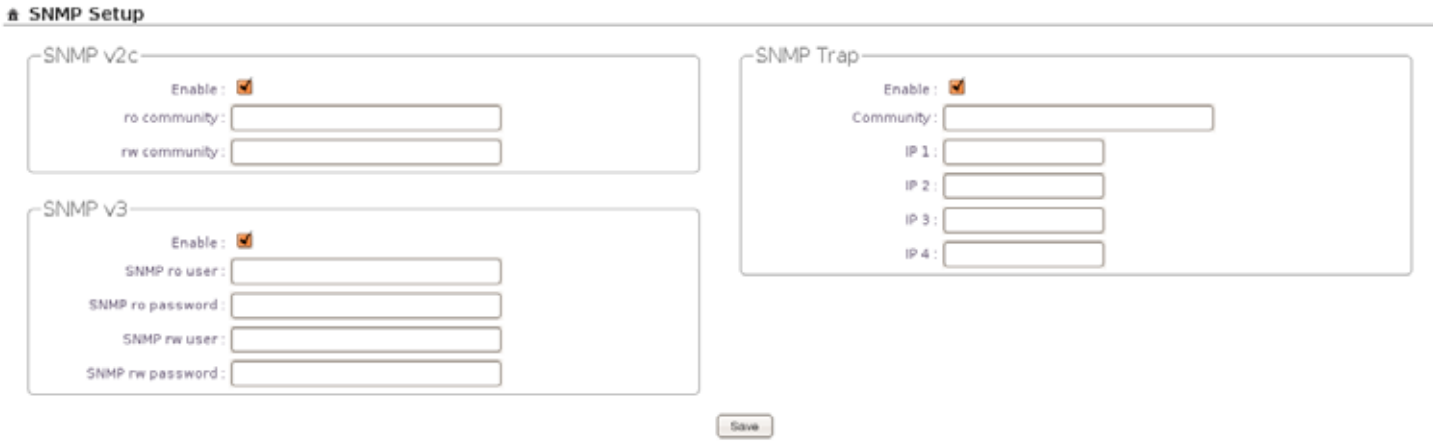
- ➔ **Enable Ping Watchdog :** control will enable Ping Watchdog Tool.
- ➔ **IP Address To Ping :** specify an IP address of the target host which will be monitored by Ping Watchdog Tool.
- ➔ **Ping Interval :** specify time interval (in seconds) between the ICMP “echo requests” are sent by the Ping Watchdog Tool. Default is **300** seconds.
- ➔ **Startup Delay :** specify initial time delay (in seconds) until first ICMP “echo requests” are sent by the Ping Watchdog Tool. The value of Startup Delay should be at least **60** seconds as the network interface and wireless connection initialization takes considerable amount of time if the device is rebooted. Default is **300** seconds.
- ➔ **Failure Count To Reboot :** specify the number of ICMP “echo response” replies. If the specified number of ICMP “echo response” packets is not received continuously, the Ping Watchdog Tool will reboot the device.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

Click “***Continue to this website***” to access the WAP-854NP's GUI. The WAP-854NP's Home page will be appear.

4.4.3 Configure SNMP

SNMP is an application-layer protocol that provides a message of format for communication between SNMP managers and agents. By enabling SNMP function, the administrator can obtain the system information remotely. Please click on **System -> SNMP Setup** and follow the below setting.



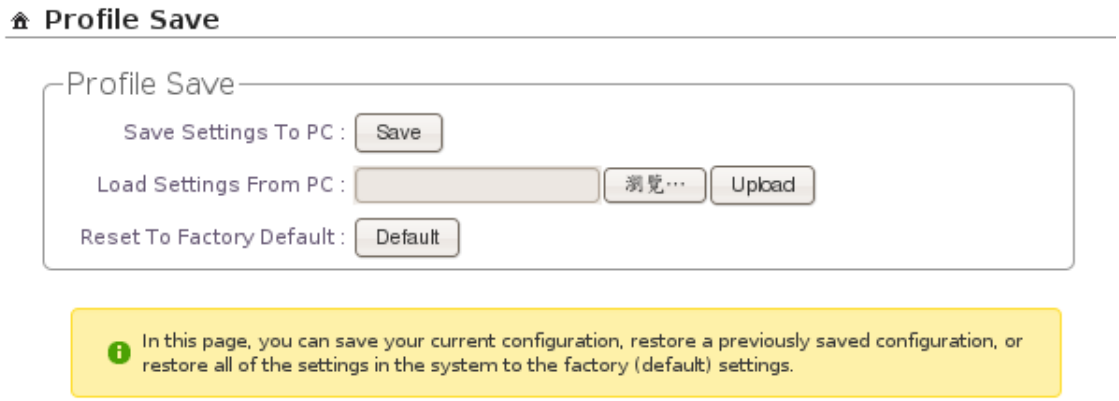
- **SNMP v2c Enable :** Check to enable SNMP v2c.
  - ➔ **ro community :** Set a community string to authorize read-only access.
  - ➔ **rw community :** Set a community string to authorize read/write access.
- **SNMP v3 Enable :** Check to enable SNMP v3.

  SNMPv3 supports the highest level SNMP security.
  - ➔ **SNMP ro user :** Set a community string to authorize read-only access.
  - ➔ **SNMP ro password :** Set a password to authorize read-only access.
  - ➔ **SNMP rw user :** Set a community string to authorize read/write access.
  - ➔ **SNMP rw password :** Set a password to authorize read/write access.
- **SNMP Trap :** Events such as cold start, interface up & down, and association & disassociation will report to an assigned server.
  - ➔ **Community :** Set a community string required by the remote host computer that will receive trap messages or notices send by the system.
  - ➔ **IP :** Enter the IP addresses of the remote hosts to receive trap messages.

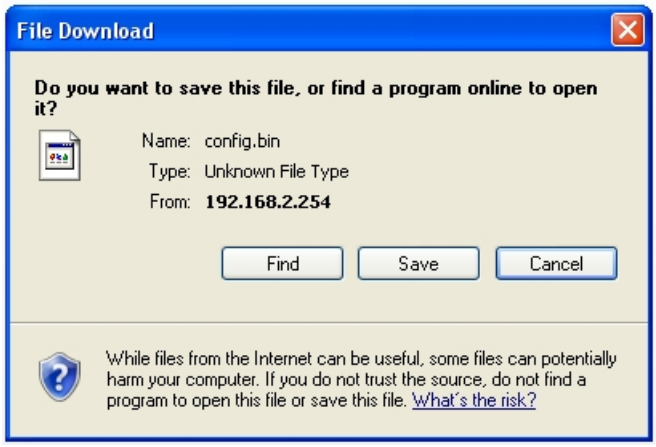
Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

4.4.4 Backup / Restore and Reset to Factory

Current settings on the system can be backed up, or previous backed up settings can be restored as well as resetting the system back to factory default can be performed via this page. Please click on **Utilities -> Profile Setting** and follow the below setting.


Profile Save
Profile Save
Save Settings To PC :
Save
Load Settings From PC :
浏览...
Upload
Reset To Factory Default :
Default
In this page, you can save your current configuration, restore a previously saved configuration, or restore all of the settings in the system to the factory (default) settings.

- **Save Settings To PC :** Click ***Save*** button to save the current configuration and **database** to a local disk.

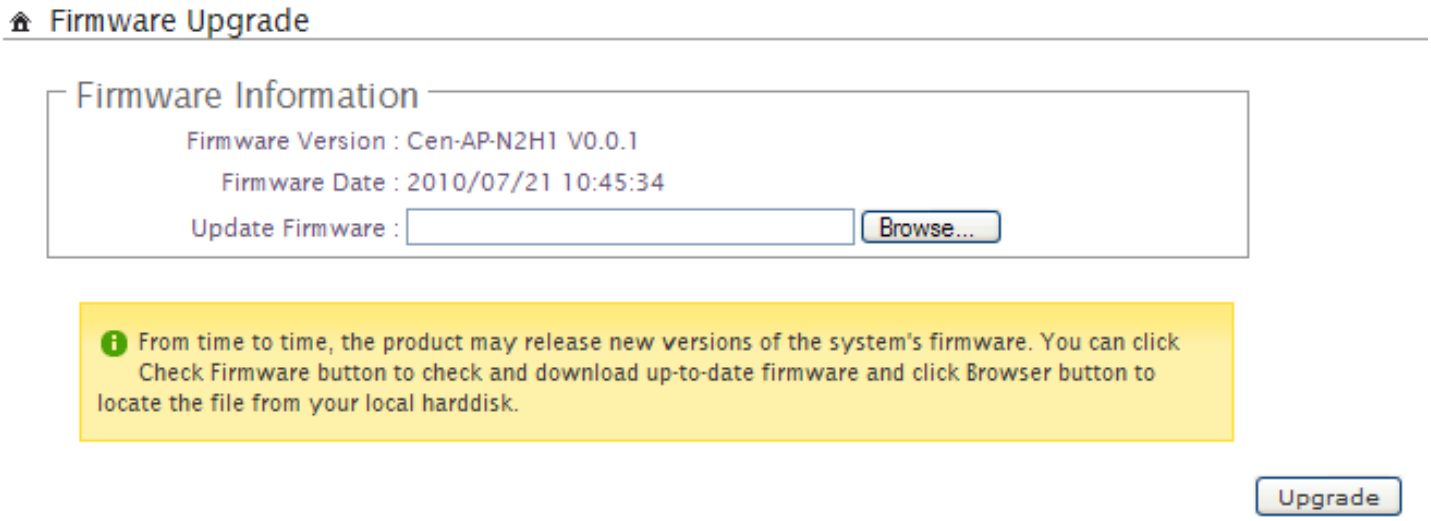

File Download
Do you want to save this file, or find a program online to open it?
Name: config.bin
Type: Unknown File Type
From: 192.168.2.254
Find
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

- **Load Settings from PC :** Click ***Browse*** button to locate a configuration file and database to restore, and then click ***Upload*** button to upload. The system will **restart** after uploading configuration and database.

- **Reset To Factory Default :** Click ***Default*** button to reset back to the factory default settings. The system will **restart** after uploading configuration and database.

4.4.5 Firmware Upgrade

The administrator can download the latest firmware from website and upgrade the system here. Click "**Browser...**" button to search for the firmware file and click "**Upgrade**" button for the firmware upgrade. It might take a few minutes before the upgrade process completes and the system needs to be restarted to activate the new firmware.

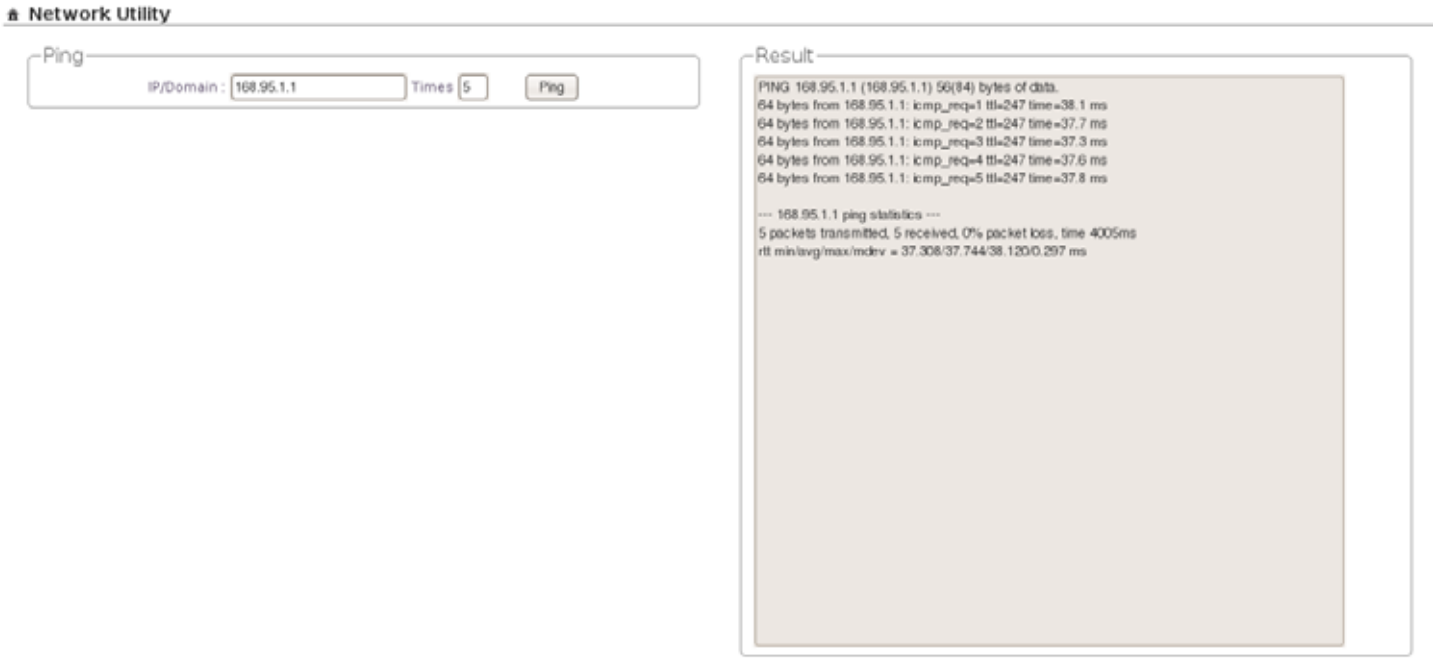

Firmware Upgrade
Firmware Information
Firmware Version : Cen-AP-N2H1 V0.0.1
Firmware Date : 2010/07/21 10:45:34
Update Firmware :
Browse...
From time to time, the product may release new versions of the system's firmware. You can click Check Firmware button to check and download up-to-date firmware and click Browser button to locate the file from your local harddisk.
Upgrade

1. To prevent data loss during firmware upgrade, please backup current settings before proceeding
2. Do not interrupt during firmware upgrade including power on/off as this may damage system.
3. Never perform firmware upgrade over wireless connection or via remote access connection.

4.4.6 Network Utility

The administrator can diagnose network connectivity via the PING utility.

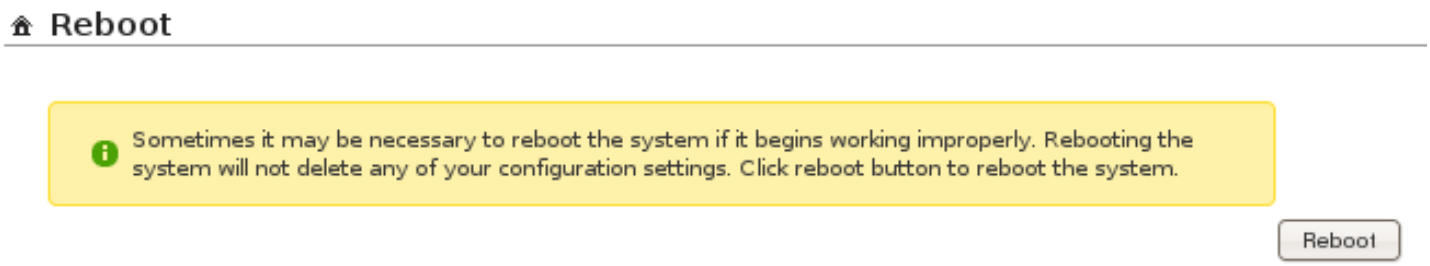
Please click on **Utilities -> Network Utility** and follow the below setting.


Network Utility
Ping
IP/Domain : 168.95.1.1
Times 5
Ping
Result
PING 168.95.1.1 (168.95.1.1) 56(84) bytes of data.
64 bytes from 168.95.1.1: icmp_req=1 ttl=247 time=38.1 ms
64 bytes from 168.95.1.1: icmp_req=2 ttl=247 time=37.7 ms
64 bytes from 168.95.1.1: icmp_req=3 ttl=247 time=37.3 ms
64 bytes from 168.95.1.1: icmp_req=4 ttl=247 time=37.6 ms
64 bytes from 168.95.1.1: icmp_req=5 ttl=247 time=37.8 ms
--- 168.95.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 37.308/37.744/38.120/0.297 ms

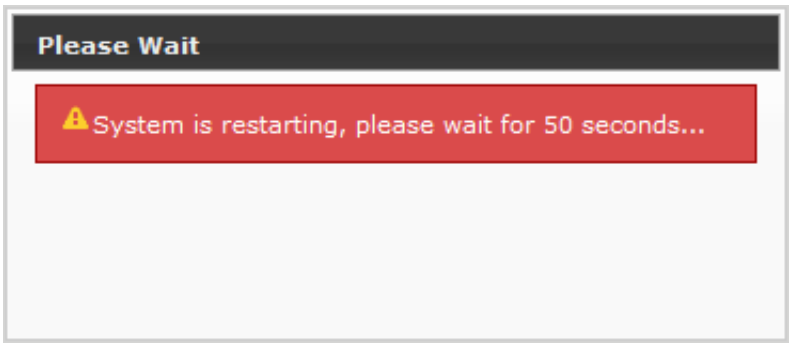
- **Ping :** This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the ***Result*** field while running the PING test.
  - **Destination IP/Domain :** Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click ***ping*** button to proceed. The ping result will be shown in the **Result** field.
  - **Times :** By default, it's 5 and the range is from 1 to 60. It indicates number of connectivity test.

4.4.7 Reboot

This function allows administrator to restart system with existing or most current settings when changes are made. Click ***Reboot*** button to proceed and take around three minutes to complete.


Reboot
Sometimes it may be necessary to reboot the system if it begins working improperly. Rebooting the system will not delete any of your configuration settings. Click reboot button to reboot the system.
Reboot

A reminder will be available for remaining time to complete. If power cycle is necessary, please wait till completion of the reboot process.

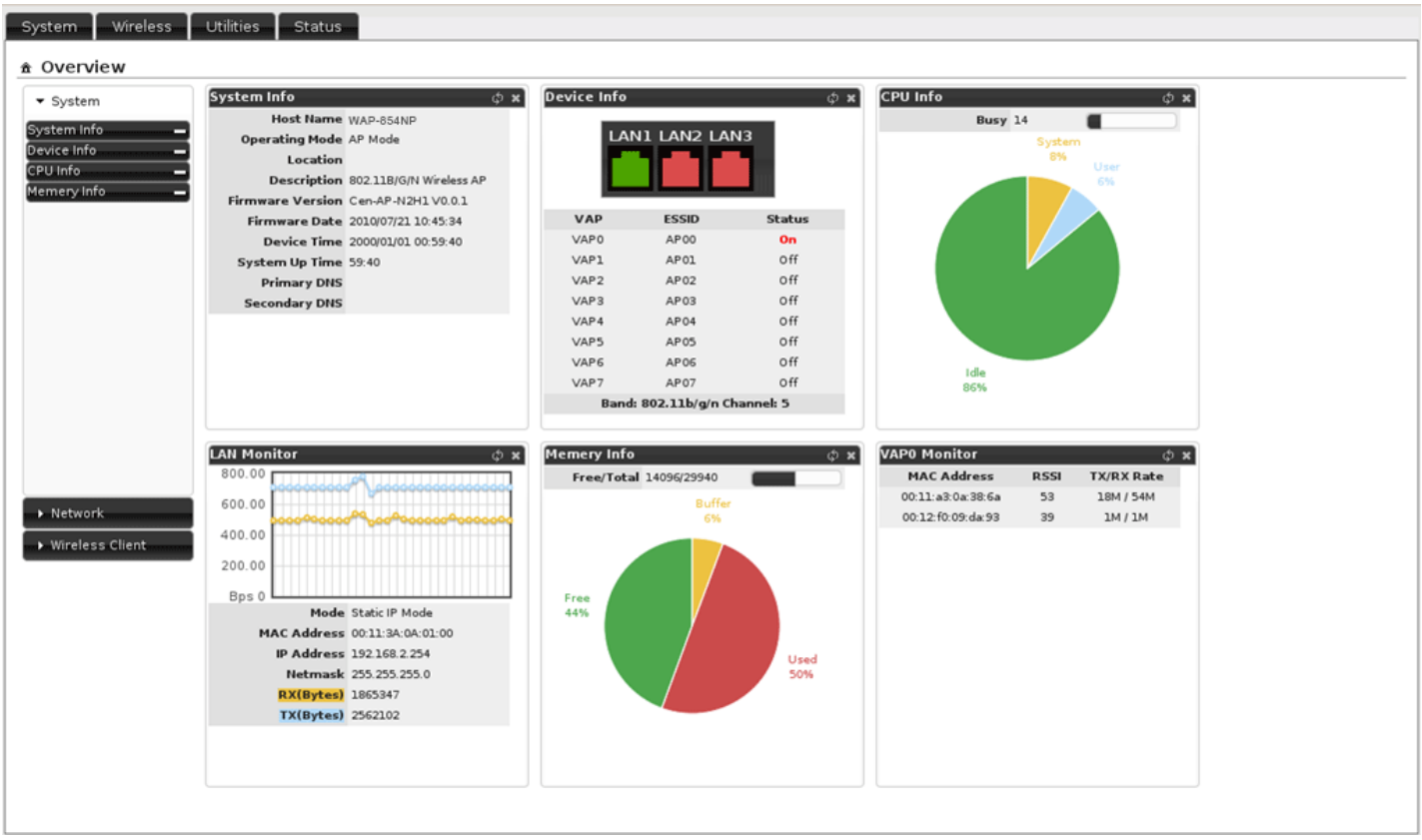


The **Home** page appears upon the completion of reboot.

4.5 Observer the Status

4.5.1 Overview

Detailed information on **System**, **Network** and **Wireless Client** can be reviewed via this page.



- **System Information :** Display the information of the system.
- **Networking Information :** Display the information of the network.
- **Wireless Client Information** : Display the information of the wireless clients.

4.5.2 Extra Info

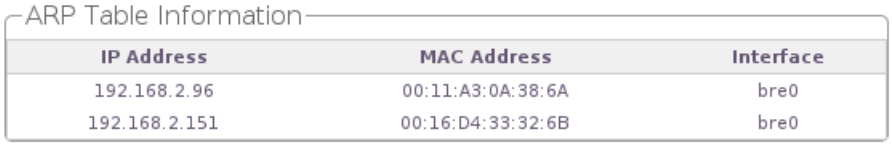
Administrator could pull out information such as Route table, ARP table, MAC table, Bridge table or STP available in the drop-down list from system. The "**Refresh**" button is used to retrieve latest table information.

- **Route Information :** Select "**Route Information**" on the drop-down list to display route table.

WAP-854NP could be used as a L2 or L3 device. It doesn't support dynamic routing protocols such as RIP or OSPF. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of system's interfaces. When used as a L2 device, it could switch packets and, as L3 device, it's capable of being a gateway to route packets inward and outward.

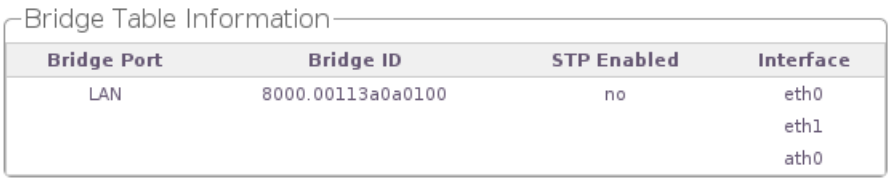
- **ARP Table Information :** Select "**ARP Table Information**" on the drop-down list to display ARP table.

ARP associates each IP address to a unique hardware address (MAC) of a device. It is important to have a unique IP address as final destination to switch packets to.



- **Bridge Table Information :** Select "**Bridge Table Information**" on the drop-down list to display bridge table.

Bridge table will show Bridge ID and STP's Status on the each Ethernet bridge and its attached interfaces, the Bridge Port should be attached to some interfaces (e.g. eth0, eth1, ath0~ath7).



- **Bridge MACs Information:** Select "**Bridge MACs Information**" on the drop-down list to display MAC table.

This table displays local MAC addresses associated with wired or wireless interfaces, but also remember non-local MAC addresses learned from wired or wireless interfaces.

Ageing timers will be reset when existing MAC addresses in table are learned again or added when new MAC addresses are seen from wired or wireless interfaces as well. When time runs out for a particular entry, it will be pruned from the table. In that situation, switching packet to that particular MAC address will be dropped.

Bridge MACs Information

Port	MAC Address	Local	Ageing Timer
LAN	00:03:7f:33:66:00	no	57.66
LAN	00:11:22:33:44:55	no	55.67
LAN	00:11:3a:0a:01:00	yes	0.00
WLAN	00:11:3a:0a:01:01	yes	0.00
WLAN	00:11:3a:0a:01:02	yes	0.00
WLAN	00:11:a3:0a:38:6a	no	20.36
LAN	00:11:a3:1b:3e:d9	no	56.62
LAN	00:12:cf:51:ea:27	no	23.94
WLAN	00:12:f0:09:da:93	no	269.59
LAN	00:15:f2:d9:a3:fd	no	175.94
LAN	00:16:d4:33:32:6b	no	0.02
LAN	00:1a:4b:1e:e5:15	no	200.03
LAN	00:d0:41:ae:36:61	no	0.06

- **Bridge STP Information :** Select "**Bridge STP Information**" on the drop-down list to display a list of bridge STP information.

Bridge STP Information

LAN			
bridge id	8000.00113a0a0100		
designated root	8000.00113a0a0100		
root port	0	path cost	0
max age	20.00	bridge max age	20.00
hello time	2.00	bridge hello time	2.00
forward delay	0.00	bridge forward delay	0.00
ageing time	300.00	gc interval	0.00
hello timer	1.87	tcn timer	0.00
topology change timer	0.00	gc timer	261.11
flags			

eth0 (1)			
port id	8001	state	forwarding
designated root	8000.00113a0a0100	path cost	100
designated bridge	8000.00113a0a0100	message age timer	0.00
designated port	8001	forward delay timer	0.00
designated cost	0	hold timer	0.87
flags			

eth1 (2)			
port id	8002	state	disabled
designated root	8000.00113a0a0100	path cost	100
designated bridge	8000.00113a0a0100	message age timer	0.00
designated port	8002	forward delay timer	0.00
designated cost	0	hold timer	0.00
flags			

ath0 (3)			
port id	8003	state	forwarding
designated root	8000.00113a0a0100	path cost	100
designated bridge	8000.00113a0a0100	message age timer	0.00
designated port	8003	forward delay timer	0.00
designated cost	0	hold timer	0.87
flags			

4.5.3 Event Log

The Event log displays system events when system is up and running. Also, it becomes very useful as a troubleshooting tool when issues are experienced in system.

- **Time :** The date and time when the event occurred.
- **Facility :** It helps users to identify source of events such “System” or “User”
- **Severity :** Severity level that a specific event is associated such as “info”, “error”, “warning”, etc.
- **Message :** Description of the event.

Click ***Refresh*** button to renew the log, or click ***Clear*** button to clear all the record.

Chapter 5. WDS Mode Configuration

This section provides detailed explanation for users to configure in the WDS mode with help of illustrations. In the WDS mode, functions listed in the table below are also available from the Web-based GUI interface.

Option	System	Wireless	Utilities	Status
Functions	Operating Mode	General Setup	Profiles Settings	System Overview
	LAN	Advanced Setup	Firmware Upgrade	Extra Info
	Management	WDS Setup	Network Utility	Event Log
	Time Server	WDS Status	Reboot	
	SNMP			

Table 5-1: WDS Mode Functions

5.1 Connect WAP-854NP to the Wired Local Network

5.1.1 Network Requirement

You could expand your Ethernet network via WDS link. In this mode, the WAP-854NP connects directly to a wired LAN, and wirelessly bridges to a remote access point via a WDS link as shown in Figure 5-1. In the mode, it can't associate with any wireless clients.

Figure 5-1 Point to Point network Configuration

5.1.2 Configure LAN Port

Here is instruction for how to setup the LAN. The connection types for LAN port : **Static IP** and **Dynamic IP**, Please click on **System -> LAN** and follow the below setting.

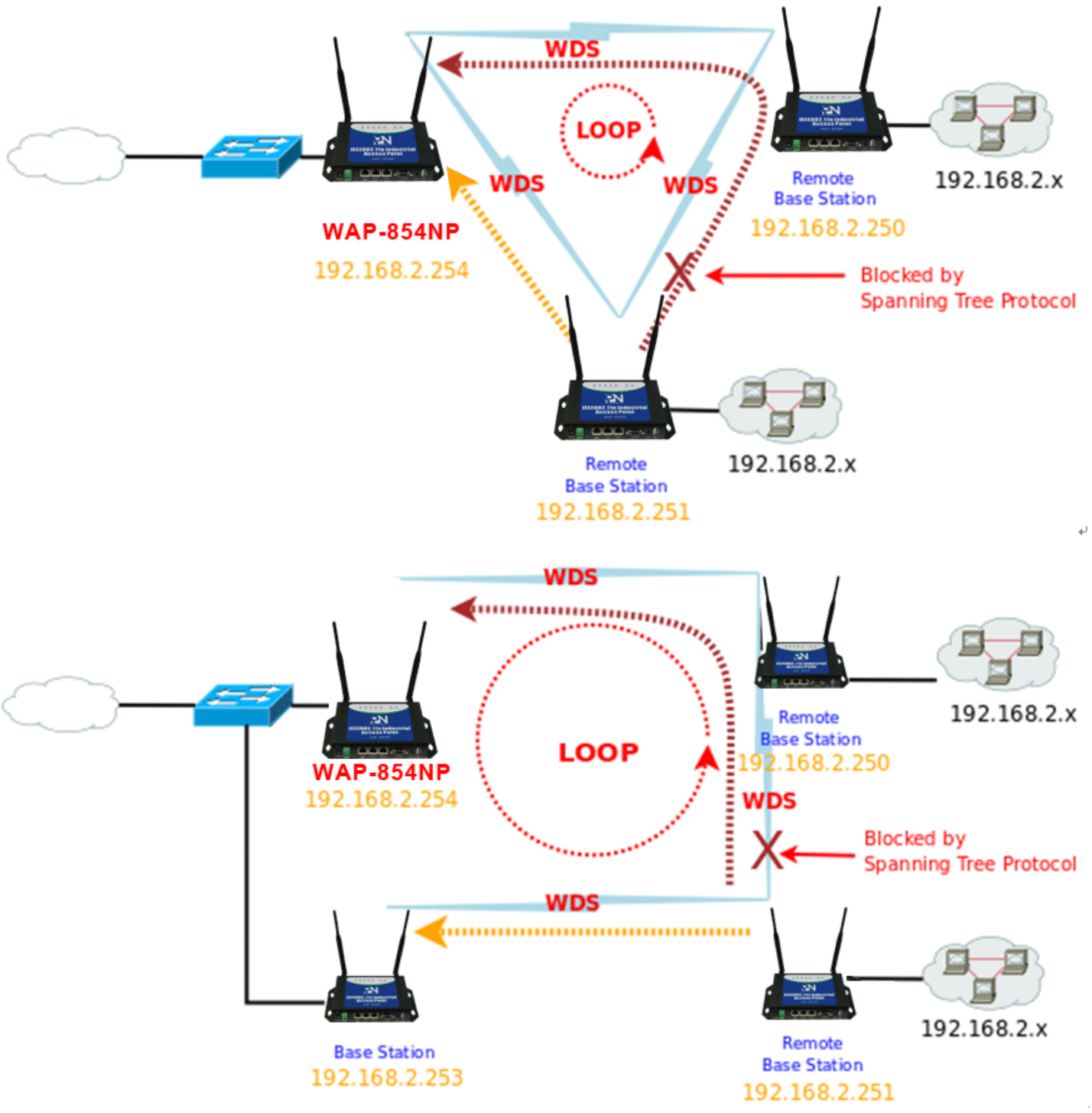
- **Mode :** Check either “Static IP” or “Dynamic IP” button as desired to set up the system IP of LAN port .
  - ➔ **Static IP :** The administrator can manually setup the LAN IP address when static IP is available/ preferred.
    - ✓ **IP Address :** The IP address of the LAN port; default IP address is 192.168.2.254
    - ✓ **IP Netmask :** The Subnet mask of the LAN port; default Netmask is 255.255.255.0
    - ✓ **IP Gateway :** The default gateway of the LAN port; default Gateway is 192.168.2.1
  - ➔ **Dynamic IP :** This configuration type is applicable when the WCB1200H5PX is connected to a network with the presence of a DHCP server; all related IP information will be provided by the DHCP server automatically.

    - ✓ **Hostname :** The Hostname of the LAN port

- **DNS :** Check either “No Default DNS Server” or “Specify DNS Server IP” button as desired to set up the system DNS.
  - **Primary :** The IP address of the primary DNS server.
  - **Secondary :** The IP address of the secondary DNS server.

- **802.1d Spanning Tree**

The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 8 WDS interfaces from WDS0 to WDS7. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d. The Spanning tree always enabled on WAP-854NP. Below Figures depict a loop for a bridged LAN between LAN and WDS link



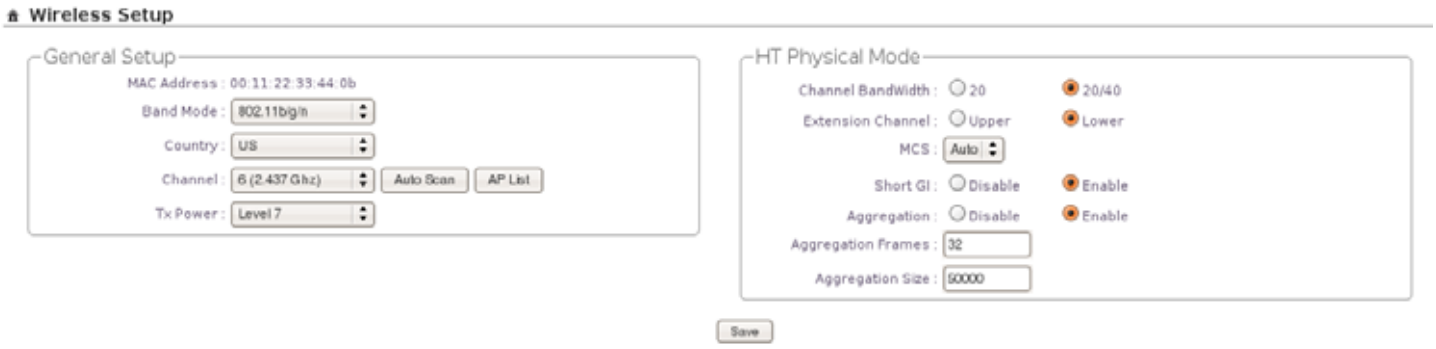
Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

5.2 Expand Your Wireless Network

The system manager can configure related wireless settings, **General Settings, Advanced Settings, WDS Setup** and **WDS Status**.

5.2.1 Configure Wireless General Setup

The administrator can change the data transmission, channel and output power settings for the system. Please click on **Wireless -> General Setup** and follow the below setting.



- **MAC address :** The MAC address of the Wireless interface is displayed here.
- **Band Mode :** Select an appropriate wireless band; bands available are 801.11b, 802.11b/g, 802.11b/g/n and 802.11n.
- **Transmit Rate Control :** Select the desired rate from the drop-down list; the options are auto or ranging from 1Mbps to 54Mbps for 802.11b/g modes, or 1Mbps to 11Mbps for 802.11b mode.
- **Country :** Select the desired country code from the drop-down list; the options are US, ETSI and Japan.
- **Channel :** The channel range will be changed by selecting different country code. The channel range from **1** to **11** for **US** country code, or **1** to **13** for **ETSI** country code, or **1** to **14** for Japan(Channel **14** only for **802.11b** Rate).

Click “**Auto Scan**”, the channel will change to next channel. Click “**AP List**” button, the system will show current all AP list.

AP Site Survey List

ESSID	MAC Address	Channel	Signal Level	Security Type
AP00	00:11:22:33:44:03	6	-1 dBm	None
MENTHOLATUM	00:11:22:5A:5B:5E	11	-1 dBm	WEP
MENTHOLATUM2	06:11:22:5A:5B:5E	11	-1 dBm	WEP
				Current Frequency:2.437 GHz (Channel 6)

Rescan Close

- **Tx Power :** You can adjust the output power of the system to get the appropriate coverage for your wireless network. Select LEVEL 1 to LEVEL 7 needed for your environment. If you are not sure of which setting to choose, then keep the default setting, **LEVEL 7**.

When **Band Mode** select in **802.11b/gn or 802.11n**, the **HT Physical Mode** settings should be show immediately.

- **Channel Bandwidth :** The "**20/40**" MHz option is usually best. The other option is available for special circumstances.
- **Extension Channel :** Only for Channel Bandwidth "**40**" MHz. Select the desired channel bonding for control.
- **MCS :** This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
- **Shout GI :** Short Guard Interval, by default, it's "Enable". it's can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **Aggregation :** By default, it's "Enable". To "Disable" to deactivated Aggregation.

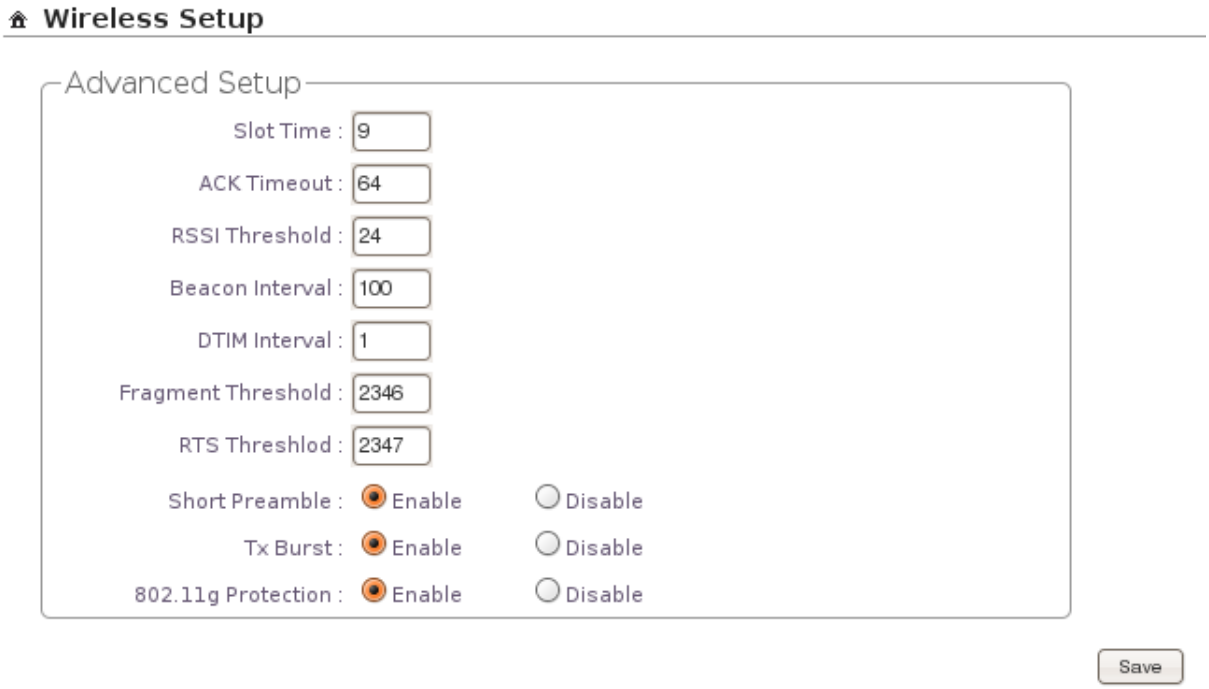
A part of the 802.11n standard (or draft-standard). It allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header.

- Aggregation Frames : The Aggregation Frames is in the range of **2~64**, default is **32**. It determines the number of frames combined on the new larger frame.
- Aggregation Size : The Aggregation Size is in the range of **1024~65535**, default is **50000**. It determines the size (in Bytes) of the larger frame.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes. The items in this page is for AP's RF general settings and will be applied to **all WDS Link**.

5.2.2 Configure Wireless Advanced Setup

The administrator can change the Slot Time, ACK Timeout, RTS threshold and fragmentation threshold settings for the system. Please click on **Wireless -> Advanced Setup** and follow the below setting.



- **Slot Time :** Slot time is in the range of **9~1489** and set in unit of ***microsecond***. The default value is **9** microsecond.

  Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. For a sender and receiver own right of the channel the shorter slot time help manage shorter wait time to re-transmit from collision because of hidden wireless clients or other causes. When collision sources can be removed sooner and other senders attempting to send are listening the channel(CSMA/CA) the owner of the channel should continue ownership and finish their transmission and release the channel. Then, following ownership of the channel will be sooner for the new pair due to shorter slot time. However, when long duration of existing collision sources and shorter slot time exist the owners might experience subsequent collisions. When adjustment to longer slot time can't improve performance then RTS/CTS could supplement and help improve performance.

- **ACK Timeout :** ACK timeout is in the range of **1~372** and set in unit of ***microsecond***. The default value is **64** microsecond.

  All data transmission in 802.11b/g request an "Acknowledgement" (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as "ACK Timeout".

ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to “Resend” packet before ACK is received, and throughput become low due to excessively high re-transmission.

ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor performance the ACK Timeout could be made longer to accommodate.

Slot Time and ACK Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

- **RSSI Threshold :** RSSI(Received Signal Strength Indication) Threshold is in the range of **-127 ~ 128**. The default value is **24**. RSSI Threshold can be used to control the level of noise received by the device.
- **Beacon Interval :** Beacon Interval is in the range of **40**~**3500** and set in unit of *millisecond*. The default value is **100** msec.

  Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called “Beacon”. Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate.

  All the radio stations received beacon recognizes the existence of such AP, and may proceed next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.

  By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.
- **DTIM Interval :** The DTIM interval is in the range of **1**~**255**. The default is **1**.

  DTIM is defined as *Delivery Traffic Indication Message*. It is used to notify the wireless stations, which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.

  A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.

- **Fragment Threshold :** The Fragment Threshold is in the range of **256**~**2346** byte. The default is **2346** byte.

  Each Wi-Fi packet can be divided into smaller packets, marked with a sequential fragment number and re-assemble in the receiving ends. The purpose is to make a short frame, instead of long frame, transmitting by radio in a heavy noisy environment. Because of sending smaller frames, corruptions are much less likely to occur. The pros is obvious, the cons is the overhead for transmission. So, in a clean environment, higher fragment threshold can be an option to increase throughput.

  Fragmentation will be triggered by setting the Fragment Threshold, usually in Byte-length. Only when the frame size is over the Threshold, fragmentation will take place automatically.

- **RTS Threshold :** TRTS Threshold is in the range of **1~2347** byte. The default is **2347** byte.

  The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.

- **Short Preamble :** By default, it's "***Enable***". To ***Disable*** is to use Long 128-bit Preamble Synchronization field.

  The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.

- **Tx Burst :** By default, it's "***Enable***". To ***Disable*** is to deactivate Tx Burst.

With TX burst enabled, AP will send many packets in a burst, without collision detection and RTS/CTS for each packet. TX Burst have better throughput but cause interference with other APs in channel.

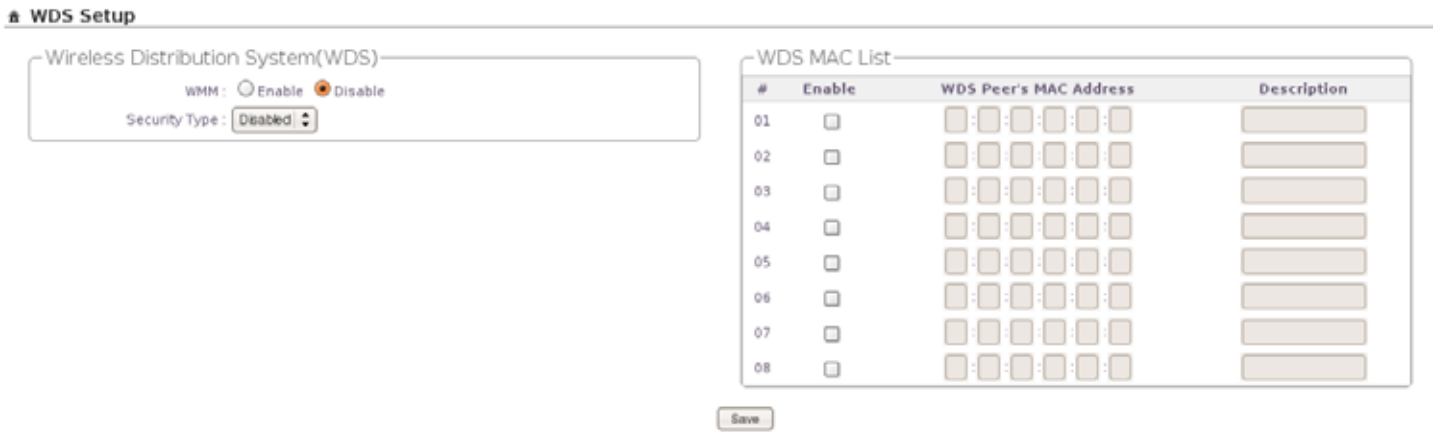
- **802.11g Protection :** Click ***Enable*** button to activate 802.11g Protection Mode, and Disable to inactivate 802.11g Protection Mode.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes. The items in this page is for AP's RF general settings and will be applied to **all WDS Link**.

5.2.3 Create WDS Link

The administrator could create WDS Links for expanding wireless network via this page. When WDS is enabled, access point functions as a wireless bridge and is able to communicate with other access points via WDS links. ***A WDS link is bidirectional and both side must support WDS. Access points know each other by MAC Address. In other words, each access point needs to include MAC address of its peer. Ensure all access points are configured with the same channel and own same security type settings.***

Please click on **Wireless -> WDS Setup** and follow the below setting.



- **WMM : Select Enable, the packets with QoS WMM has higher priority.**
- **Security Type :** Option is "**Disable**", "**WEP**" or "**AES**" from drop-down list. Needs the same type to build WDS links. Security type takes effect when WDS is enabled.
  - ➔ **WEP Key :** Enter **5 / 13 / 16 ASCII** or **10 / 26 /32 HEX** format WEP key.
  - ➔ **AES Key :** Enter **32 HEX** format AES key.

AES Encryption only support between WAP-854NP and WAP-854NP

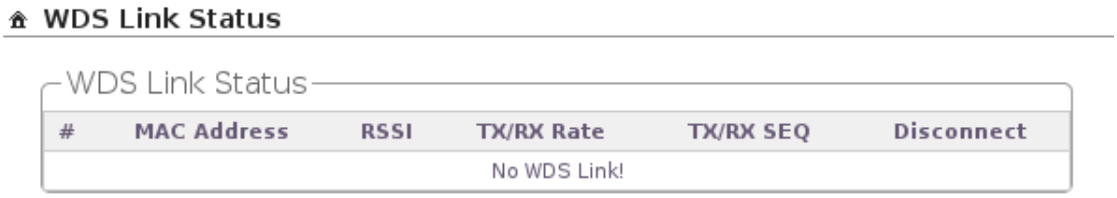
- **WDS MAC List**
  - ➔ **Enable :** Click ***Enable*** to create WDS link.
  - ➔ **WDS Peer's MAC Address :** Enter the MAC address of WDS peer.
  - ➔ **Description :** Description of WDS link.

The WDS link needs to be set at same **Channel** and **Security Type** between WDS link.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes.

5.2.4 View WDS Link Status

Peers MAC Address, antenna 0/1 received signal strength, phy mode and channel bandwidth for each WDS are available.



- **MAC Address :** Display MAC address of WDS peer.
- **RSSI :** Indicate the RSSI of the respective WDS's link.
- **TX/RX Rate :** Indicate the TX/RX Rate of the respective WDS's link.
- **TX/RX SEQ :** Indicate the TX/RX sequence of the respective WDS's link.
- **Disconnect :** Administrator can kick out a specific client, click “**Delete**” button to kick out specific WDS's link

5.3 Manage the System

5.3.1 Configure System Time

System time can be configured via this page where manual setting and NTP server configuration are both supported. Please click on **System -> Time Server** and follow the below setting.

- **Local Time :** Display the current time of the system.
- **Setup Time Use NTP :** Enable Network Time Protocol, NTP, to synchronize the system time with NTP server.
  - ➔ **Default NTP Server :** Select the NTP Server from the drop-down list.
  - ➔ **Time Zone :** Please set a time zone from where the accurate time can be supplied, **(GMT+08:00) Taipei** for example.
  - ➔ **Daylight saving time :** Enable Daylight saving time from where the accurate time needed.

If Time server setting selected in “Setup Time User NTP”, please verify system's DNS and Default Gateway setting first.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

5.3.2 Configure Management

The administrator can later obtain the geographical location of the system via the information configured here. The administrator also can change system password and configure system login methods. Please click **System -> Management** and follow the below settings.

- **System Information**
  - ➔ **System Name :** Enter a desired name or use the default provided.
  - ➔ **Description :** Denote further information of the system.
  - ➔ **Location :** Enter related geographical location information of the system; administrator/manager will be able to locate the system easily.

- **Root Password :** Log in as a root user and is allowed to change its own. Root user also can change **admin** user's and **operator** user's password. Click ***Save*** button to activate the new password.
  - ➔ **New Password :** Please input the new password of administrator.
  - ➔ **Check New Password :** Please input again the new password of administrator.

- **Admin Login Methods :** The admin manager can enable or disable system login methods, it also can change services port. Click ***Save*** button to activate the admin login methods.
  - ➔ **Enable HTTP :** Select Enable HTTP to activate HTTP Service
  - ➔ **HTTP Port :** Please input 1 ~ 65535 value to set HTTP Port; default value is **80**
  - ➔ **Enable Telnet :** Select Enable HTTP to activate HTTP Service
  - ➔ **Telnet Port :** Please input 1 ~ 65535 value to set HTTP Port; default value is **23**

- **Ping Watchdog :** The ping watchdog sets the WAP-854NP Device to continuously ping a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, the WAP-854NP device will automatically reboot. This option creates a kind of "fail-proof" mechanism.

  Ping Watchdog is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. The Ping works by sending ICMP “echo request” packets to the target host and listening for ICMP “echo response” replies. If the defined number of replies is not received, the tool reboots the device.

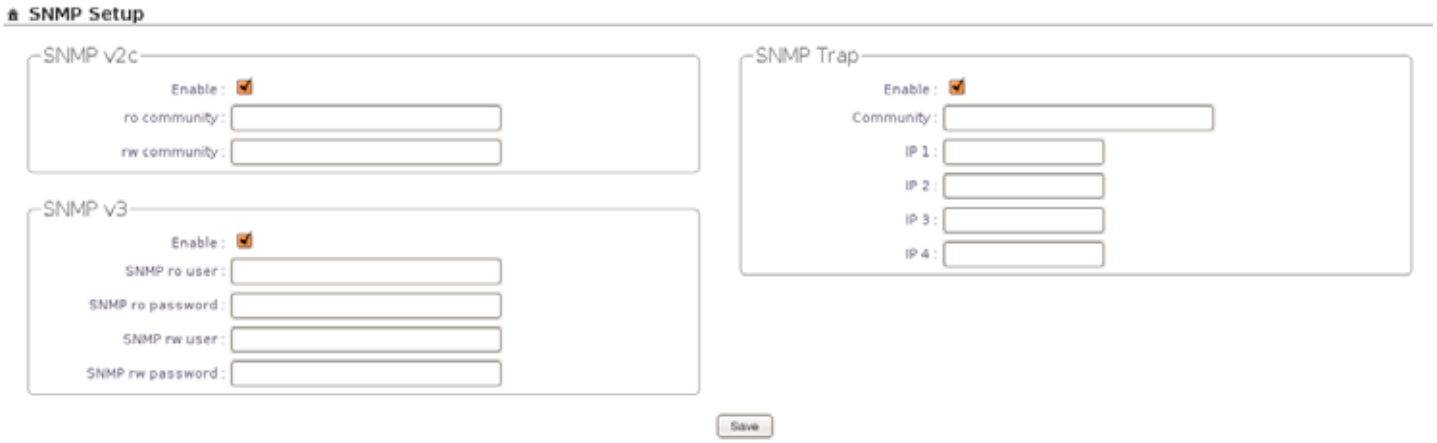
  - ➔ **Enable Ping Watchdog :** control will enable Ping Watchdog Tool.
  - ➔ **IP Address To Ping :** specify an IP address of the target host which will be monitored by Ping Watchdog Tool.
  - ➔ **Ping Interval :** specify time interval (in seconds) between the ICMP “echo requests” are sent by the Ping Watchdog Tool. Default is **300** seconds.
  - ➔ **Startup Delay :** specify initial time delay (in seconds) until first ICMP “echo requests” are sent by the Ping Watchdog Tool. The value of Startup Delay should be at least **60** seconds as the network interface and wireless connection initialization takes considerable amount of time if the device is rebooted. Default is **300** seconds.
  - ➔ **Failure Count To Reboot :** specify the number of ICMP “echo response” replies. If the specified number of ICMP “echo response” packets is not received continuously, the Ping Watchdog Tool will reboot the device.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

Click “***Continue to this website***” to access the WAP-854NP's GUI. The WAP-854NP's Home page will be appear.

5.3.3 Configure SNMP

SNMP is an application-layer protocol that provides a message of format for communication between SNMP managers and agents. By enabling SNMP function, the administrator can obtain the system information remotely. Please click on **System -> SNMP Setup** and follow the below setting.



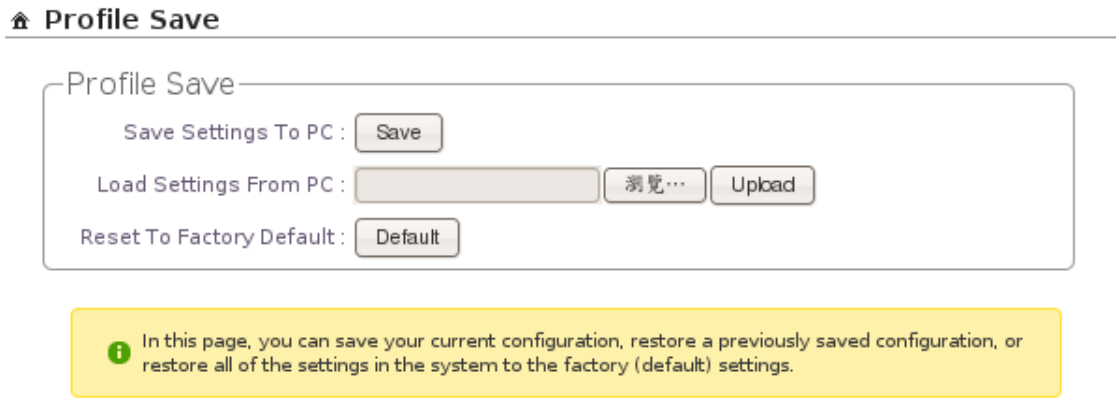
- **SNMP v2c Enable :** Check to enable SNMP v2c.
  - ➔ **ro community :** Set a community string to authorize read-only access.
  - ➔ **rw community :** Set a community string to authorize read/write access.
- **SNMP v3 Enable :** Check to enable SNMP v3.

  SNMPv3 supports the highest level SNMP security.
  - ➔ **SNMP ro user :** Set a community string to authorize read-only access.
  - ➔ **SNMP ro password :** Set a password to authorize read-only access.
  - ➔ **SNMP rw user :** Set a community string to authorize read/write access.
  - ➔ **SNMP rw password :** Set a password to authorize read/write access.
- **SNMP Trap :** Events such as cold start, interface up & down, and association & disassociation will report to an assigned server.
  - ➔ **Community :** Set a community string required by the remote host computer that will receive trap messages or notices send by the system.
  - ➔ **IP :** Enter the IP addresses of the remote hosts to receive trap messages.

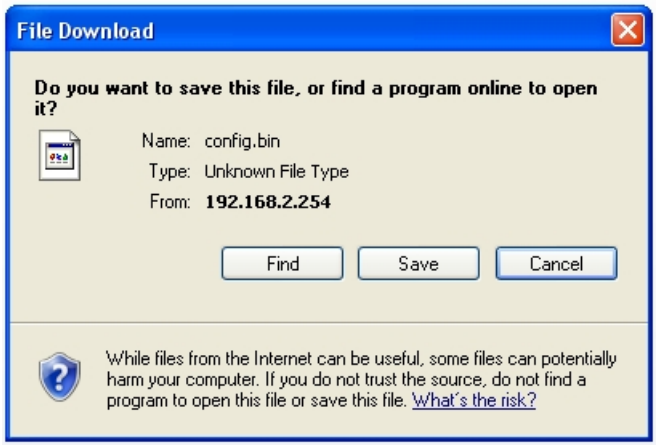
Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

5.3.4 Backup / Restore and Reset to Factory

Current settings on the system can be backed up, or previous backed up settings can be restored as well as resetting the system back to factory default can be performed via this page. Please click on **Utilities -> Profile Setting** and follow the below setting.


Profile Save
Profile Save
Save Settings To PC :
Save
Load Settings From PC :
浏览...
Upload
Reset To Factory Default :
Default
In this page, you can save your current configuration, restore a previously saved configuration, or restore all of the settings in the system to the factory (default) settings.

- **Save Settings To PC :** Click ***Save*** button to save the current configuration and **database** to a local disk.

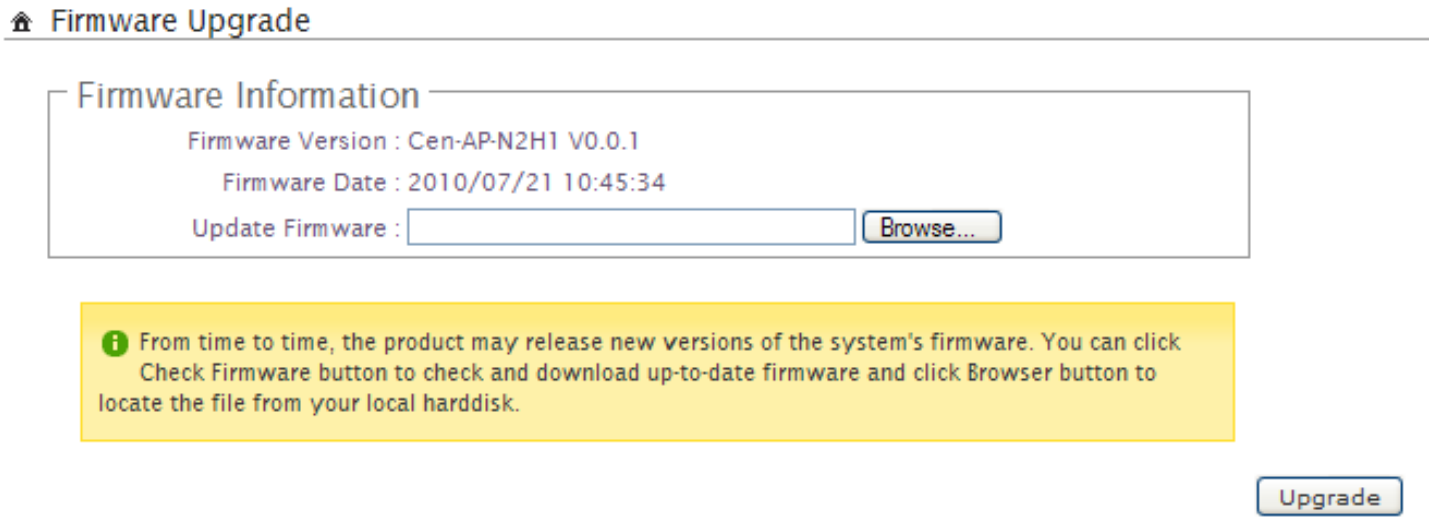

File Download
Do you want to save this file, or find a program online to open it?
Name: config.bin
Type: Unknown File Type
From: 192.168.2.254
Find
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

- **Load Settings from PC :** Click ***Browse*** button to locate a configuration file and database to restore, and then click ***Upload*** button to upload. The system will **restart** after uploading configuration and database.

- **Reset To Factory Default :** Click ***Default*** button to reset back to the factory default settings. The system will **restart** after uploading configuration and database.

5.3.5 Firmware Upgrade

The administrator can download the latest firmware from website and upgrade the system here. Click "**Browser...**" button to search for the firmware file and click "**Upgrade**" button for the firmware upgrade. It might take a few minutes before the upgrade process completes and the system needs to be restarted to activate the new firmware.

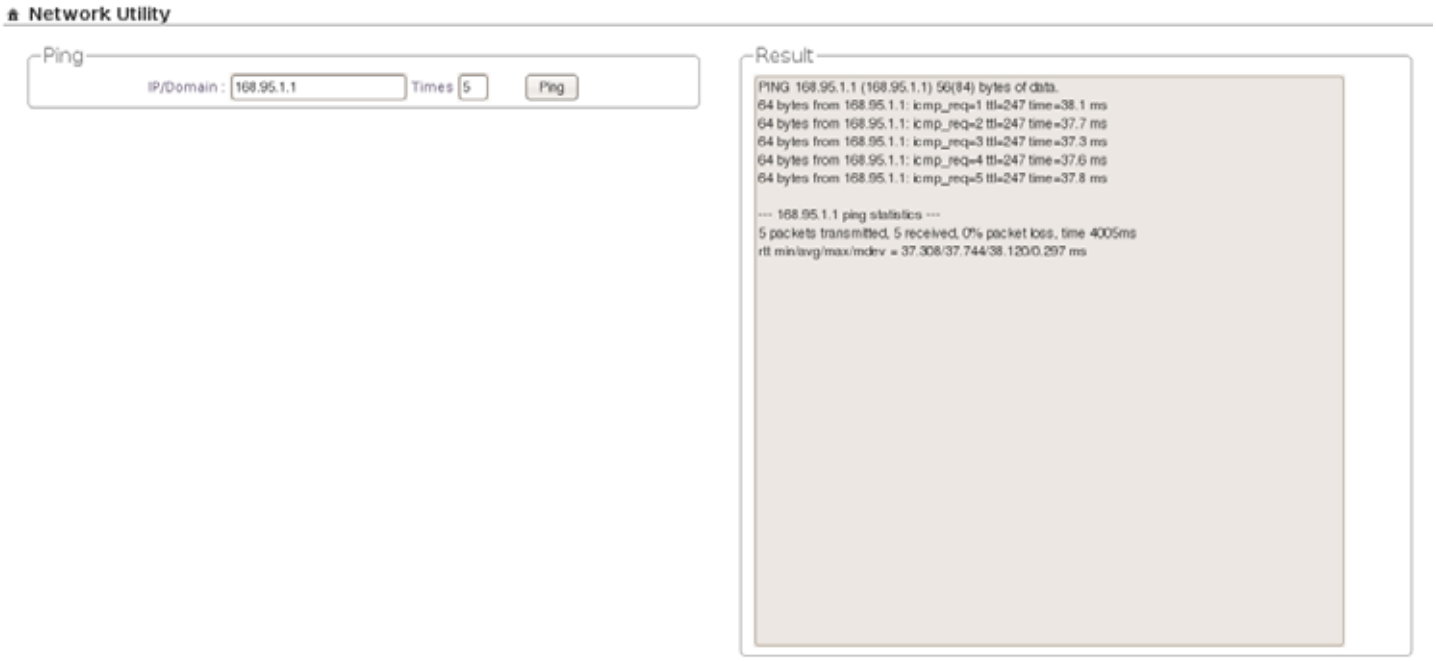

Firmware Upgrade
Firmware Information
Firmware Version : Cen-AP-N2H1 V0.0.1
Firmware Date : 2010/07/21 10:45:34
Update Firmware :
Browse...
From time to time, the product may release new versions of the system's firmware. You can click Check Firmware button to check and download up-to-date firmware and click Browser button to locate the file from your local harddisk.
Upgrade

1. To prevent data loss during firmware upgrade, please backup current settings before proceeding
2. Do not interrupt during firmware upgrade including power on/off as this may damage system.
3. Never perform firmware upgrade over wireless connection or via remote access connection.

5.3.6 Network Utility

The administrator can diagnose network connectivity via the PING utility.

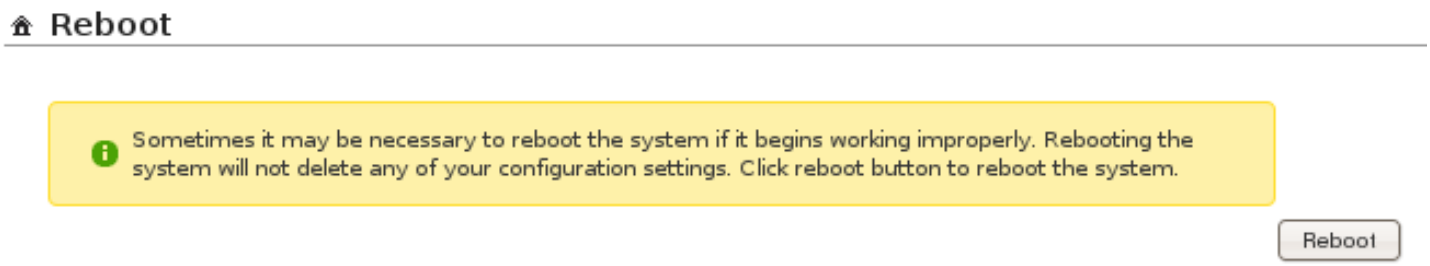
Please click on **Utilities -> Network Utility** and follow the below setting.


Network Utility
Ping
IP/Domain : 168.95.1.1
Times 5
Ping
Result
PING 168.95.1.1 (168.95.1.1) 56(84) bytes of data.
64 bytes from 168.95.1.1: icmp_req=1 ttl=247 time=38.1 ms
64 bytes from 168.95.1.1: icmp_req=2 ttl=247 time=37.7 ms
64 bytes from 168.95.1.1: icmp_req=3 ttl=247 time=37.3 ms
64 bytes from 168.95.1.1: icmp_req=4 ttl=247 time=37.6 ms
64 bytes from 168.95.1.1: icmp_req=5 ttl=247 time=37.8 ms
--- 168.95.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 37.308/37.744/38.120/0.297 ms

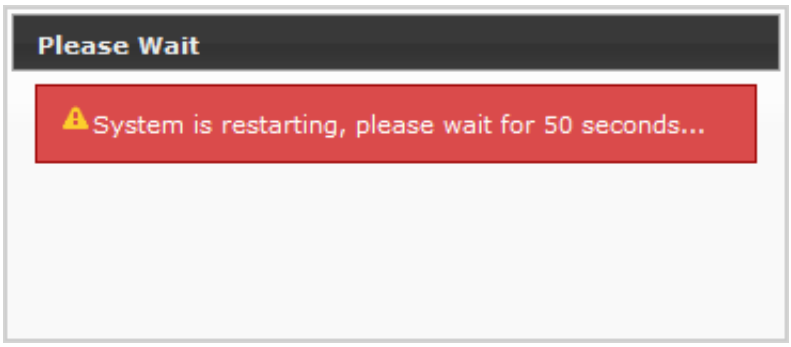
- **Ping :** This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the ***Result*** field while running the PING test.
  - **Destination IP/Domain :** Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click ***ping*** button to proceed. The ping result will be shown in the **Result** field.
  - **Times :** By default, it's 5 and the range is from 1 to 60. It indicates number of connectivity test.

5.3.7 Reboot

This function allows administrator to restart system with existing or most current settings when changes are made. Click ***Reboot*** button to proceed and take around three minutes to complete.


Reboot
Sometimes it may be necessary to reboot the system if it begins working improperly. Rebooting the system will not delete any of your configuration settings. Click reboot button to reboot the system.
Reboot

A reminder will be available for remaining time to complete. If power cycle is necessary, please wait till completion of the reboot process.

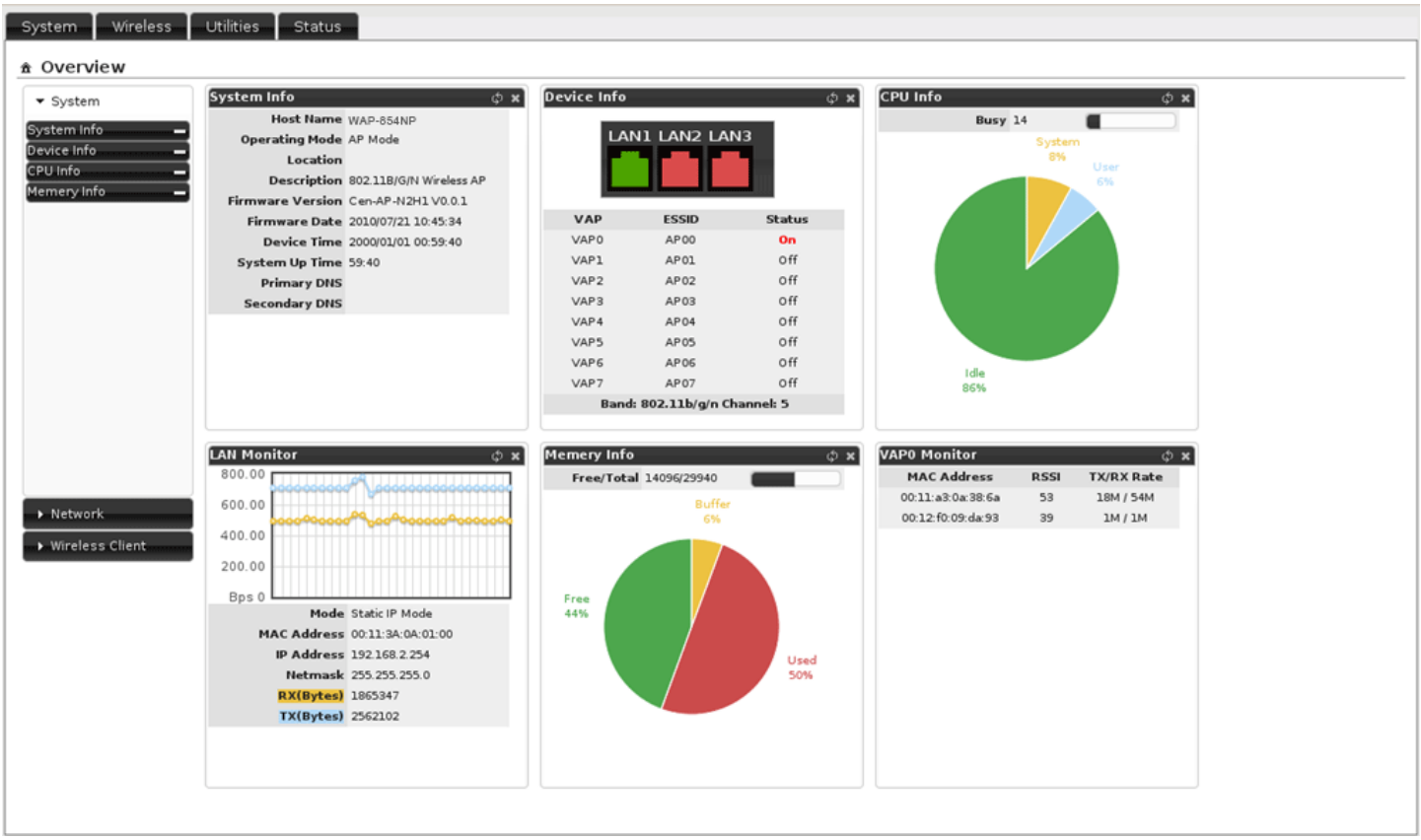


The **Home** page appears upon the completion of reboot.

5.4 Observer the Status

5.4.1 Overview

Detailed information on **System**, **Network** and **Wireless Client** can be reviewed via this page.



- **System Information :** Display the information of the system.
- **Networking Information :** Display the information of the network.
- **Wireless Client Information** : Display the information of the wireless clients.

5.4.2 Extra Info

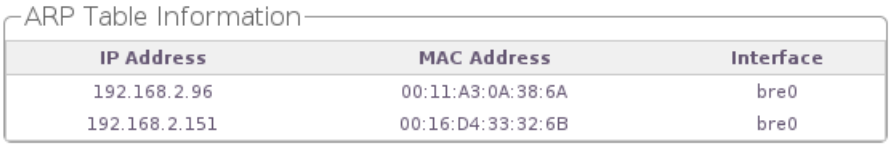
Administrator could pull out information such as Route table, ARP table, MAC table, Bridge table or STP available in the drop-down list from system. The "**Refresh**" button is used to retrieve latest table information.

- **Route Information :** Select "**Route Information**" on the drop-down list to display route table.

WAP-854NP could be used as a L2 or L3 device. It doesn't support dynamic routing protocols such as RIP or OSPF. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of system's interfaces. When used as a L2 device, it could switch packets and, as L3 device, it's capable of being a gateway to route packets inward and outward.

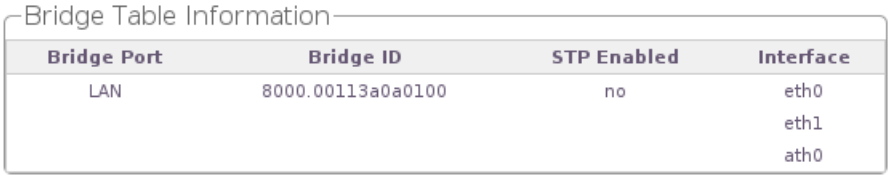
- **ARP Table Information :** Select "**ARP Table Information**" on the drop-down list to display ARP table.

ARP associates each IP address to a unique hardware address (MAC) of a device. It is important to have a unique IP address as final destination to switch packets to.



- **Bridge Table Information :** Select "**Bridge Table Information**" on the drop-down list to display bridge table.

Bridge table will show Bridge ID and STP's Status on the each Ethernet bridge and its attached interfaces, the Bridge Port should be attached to some interfaces (e.g. eth0, eth1, ath0).



- **Bridge MACs Information :** Select "**Bridge MACs Information**" on the drop-down list to display MAC table.

This table displays local MAC addresses associated with wired or wireless interfaces, but also remember non-local MAC addresses learned from wired or wireless interfaces.

Ageing timers will be reset when existing MAC addresses in table are learned again or added when new MAC addresses are seen from wired or wireless interfaces as well. When time runs out for a particular entry, it will be pruned from the table. In that situation, switching packet to that particular MAC address will be dropped.

Bridge MACs Information

Port	MAC Address	Local	Ageing Timer
LAN	00:03:7f:33:66:00	no	57.66
LAN	00:11:22:33:44:55	no	55.67
LAN	00:11:3a:0a:01:00	yes	0.00
WLAN	00:11:3a:0a:01:01	yes	0.00
WLAN	00:11:3a:0a:01:02	yes	0.00
WLAN	00:11:a3:0a:38:6a	no	20.36
LAN	00:11:a3:1b:3e:d9	no	56.62
LAN	00:12:cf:51:ea:27	no	23.94
WLAN	00:12:f0:09:da:93	no	269.59
LAN	00:15:f2:d9:a3:fd	no	175.94
LAN	00:16:d4:33:32:6b	no	0.02
LAN	00:1a:4b:1e:e5:15	no	200.03
LAN	00:d0:41:ae:36:61	no	0.06

- **Bridge STP Information :** Select "**Bridge STP Information**" on the drop-down list to display a list of bridge STP information.

Bridge STP Information

LAN			
bridge id	8000.00113a0a0100		
designated root	8000.00113a0a0100		
root port	0	path cost	0
max age	20.00	bridge max age	20.00
hello time	2.00	bridge hello time	2.00
forward delay	0.00	bridge forward delay	0.00
ageing time	300.00	gc interval	0.00
hello timer	1.87	tcn timer	0.00
topology change timer	0.00	gc timer	261.11
flags			

eth0 (1)			
port id	8001	state	forwarding
designated root	8000.00113a0a0100	path cost	100
designated bridge	8000.00113a0a0100	message age timer	0.00
designated port	8001	forward delay timer	0.00
designated cost	0	hold timer	0.87
flags			

eth1 (2)			
port id	8002	state	disabled
designated root	8000.00113a0a0100	path cost	100
designated bridge	8000.00113a0a0100	message age timer	0.00
designated port	8002	forward delay timer	0.00
designated cost	0	hold timer	0.00
flags			

ath0 (3)			
port id	8003	state	forwarding
designated root	8000.00113a0a0100	path cost	100
designated bridge	8000.00113a0a0100	message age timer	0.00
designated port	8003	forward delay timer	0.00
designated cost	0	hold timer	0.87
flags			

5.4.3 Event Log

The Event log displays system events when system is up and running. Also, it becomes very useful as a troubleshooting tool when issues are experienced in system.

- **Time :** The date and time when the event occurred.
- **Facility :** It helps users to identify source of events such “System” or “User”
- **Severity :** Severity level that a specific event is associated such as “info”, “error”, “warning”, etc.
- **Message :** Description of the event.

Click ***Refresh*** button to renew the log, or click ***Clear*** button to clear all the record.

Appendix A. Web GUI valid Characters

Table A Web GUI Valid Characters

Block	Field	Valid Characters
LAN	IP Address	IP Format; 1-254
	IP Netmask	128.0.0.0 ~ 255.255.255.252
	IP Gateway	IP Format; 1-254
	Hostname	Length : 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	DNS	IP Format; 1-254
Management	System Name	Length : 32 0-9, A-Z, a-z Space ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Description	Length : 45 chars Space
	Location	Length : 32 0-9, A-Z, a-z Space ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	New Password	Length : 4 ~ 30 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Check New Password	Length : 4 ~ 30 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Port	1 ~ 65535
	IP Address To Ping	IP Format; 1-254
	Ping Interval	60 ~ 3600, default is 300
	Startup Delay	60 ~ 3600, default is 300
	Failure Count To Reboot	1 ~ 99 , default is 3
SNMP	RO/ RW community	Length : 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =
	RO/ RW user	Length : 31 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =
	RO/ RW password	Length : 8 ~ 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =
	Community	Length : 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =
	IP	IP Format; 1-254

Table A Web GUI Valid Characters (continued)

Block	Field	Valid Characters
General Setup	Aggregation Frames	2-64, default is 32
	Aggregation Size	1024-65535, default is 50000
Advanced Setup	Beacon Interval	40 ~ 3500
	DTIM Interval	1 ~ 255
	Fragment Threshold	256 ~ 2346
	RTS Threshold	1 ~ 2347
Virtual AP Setup	ESSID	Length : 1-31 0-9, A-Z, a-z Space ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Maximum Clients	1 ~ 32
	WEP Key	10, 26, 32 HEX chars or 5, 13, 16 ASCII chars
	Group Key Update Period	>=10 seconds, default is 600
	Master Key Update Period	>= 10 seconds, default is 86400
	WEP Key Update Period	>=0 seconds, default is 300, 0 is disable
	Pre-Shared Key	8 ~ 63 ASCII chars; 64 HEX chars
	Radius Server IP	IP Format; 1-254
	Radius Port	1 ~ 65535
	Shared Secret	1 ~ 64 characters
	EAP Reauth Period	>= 0 seconds; 0 is disable, default is 3600
WDS Setup	WEP Key	10, 26, 32 HEX chars or 5, 13, 16 ASCII chars
	AES Key	32 Hex chars
	Peer's MAC Address	12 HEX chars
	Description	32 chars Space